ID: 635361
Sample Name:
RE_iRecord_Installer.msi
Cookbook: default.jbs
Time: 20:17:52
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

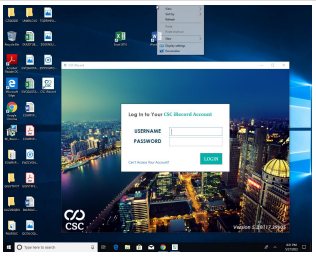
Windows Analysis Report

RE_iRecord_Installer.msi

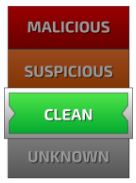
Overview

General Information

Sample Name:	RE_iRecord_Installer.msi
Analysis ID:	635361
MD5:	fd867ada4f27257.
SHA1:	ef352d9be1ba30..
SHA256:	609053e562cd36..
Infos:	



Detection



Score:	4
Range:	0 - 100
Whitelisted:	false
Confidence:	0%

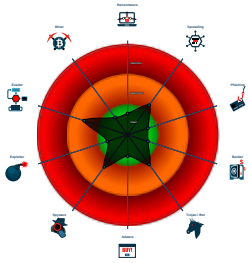
Compliance

Score:	32
Range:	0 - 100

Signatures

- Queries the volume information (nam…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Creates files inside the system direc…
- Stores files to the Windows start me…
- JA3 SSL client fingerprint seen in co…
- Found dropped PE file which has no…
- PE file contains executable resourc…
- IP address seen in connection with …
- Contains long sleeps (>= 3 min)
- Enables debug privileges
- Creates a DirectInput object (often f…
- EXE planting / hijacking vulnerabiliti…

Classification



Analysis Advice

- **Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox**
- **Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook**
- **Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior**
- **Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")**
- **Sample searches for specific file, try point organization specific fake files to the analysis machine**

Process Tree

- **System is w10x64**
- msiexec.exe (PID: 6632 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\RE_iRecord_Installer.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 6692 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 6960 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 5E1FB7355188E254823CE3315A71CFED C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - iRecord_WPF.exe (PID: 7048 cmdline: C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe MD5: 211ED9D4E17D3FED889A73CA6065FC69)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Compliance

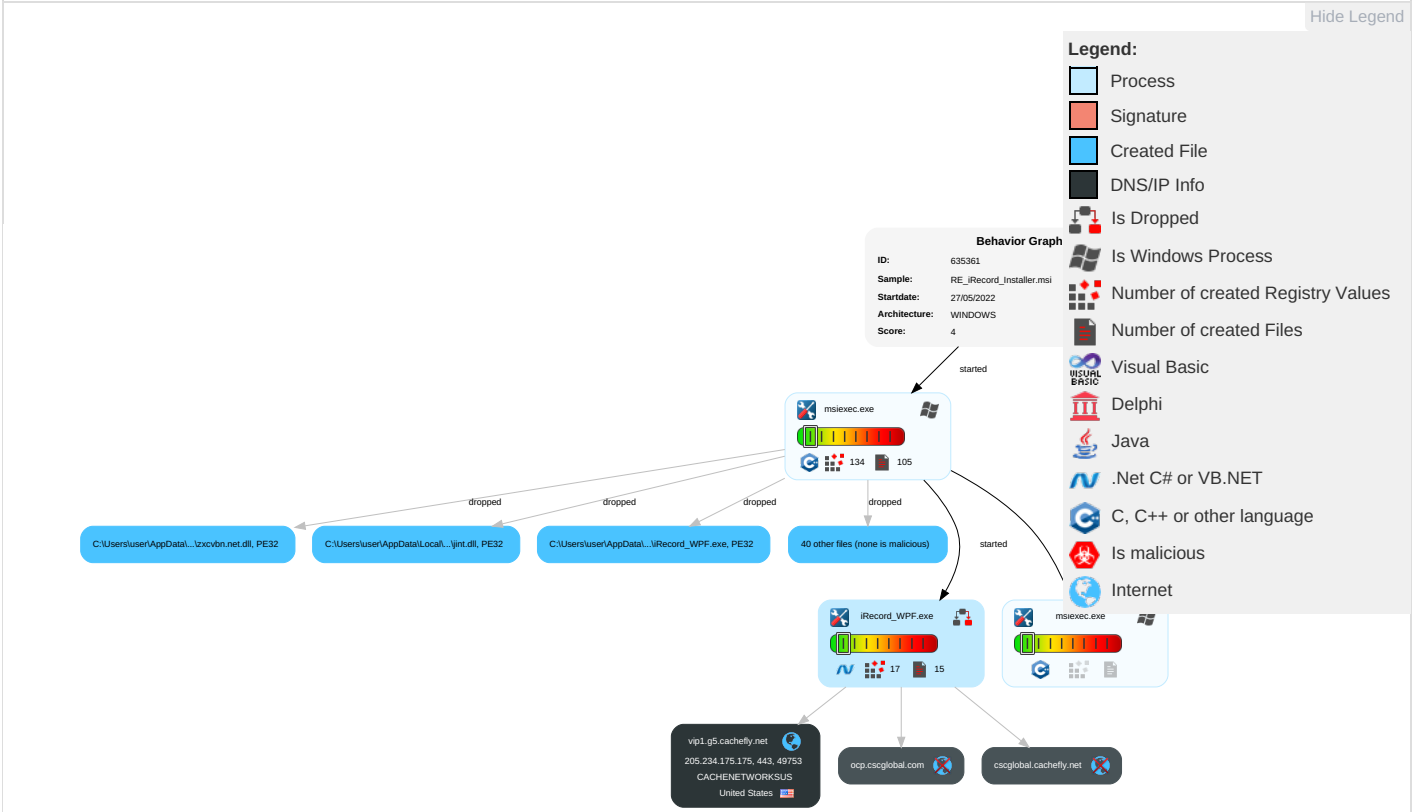
EXE planting / hijacking vulnerabilities found
DLL planting / hijacking vulnerabilities found
Uses secure TLS version for HTTPS connections
PE / OLE file has a valid certificate
Binary contains paths to debug symbols

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Process Injection	1 1 Masqueradi ng	1 Input Capture	1 Security Software Discovery	1 Replication Through Removable Media	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	1 1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	2 DLL Search Order Hijacking	1 DLL Side-Loading	2 1 Virtualizatio n/Sandbox Evasion	Security Account Manager	2 1 Virtualizatio n/Sandbox Evasion	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	2 DLL Search Order Hijacking	1 Process Injection	NTDS	1 1 Peripheral Device Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 DLL Search Order Hijacking	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

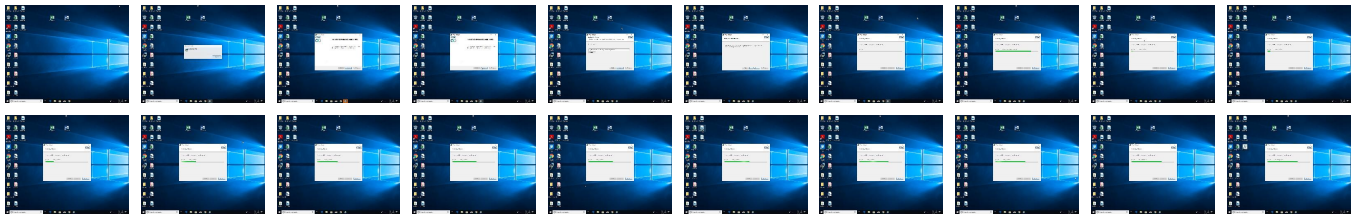
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Programs\CSC\iRecord\BarcodeLib.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Programs\CSC\iRecord\BarcodeLib.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\ClearScript.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.barcode.1d.reader.64.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.barcode.1d.reader.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.filters.64.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.filters.64.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.filters.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.filters.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.image.gdimgplug.64.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.image.gdimgplug.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.image.gdimgplug.dll	3%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.gemedicalsystems.com/it_solutions/rad_pacs/	0%	Virustotal		Browse
http://www.gemedicalsystems.com/it_solutions/rad_pacs/	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetConnectorTransactionXmlByCountyGuidAndErIDT	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetDemoXmlResponse	0%	Avira URL Cloud	safe	
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.SynchData/Service.asmx	0%	Avira URL Cloud	safe	
http://https://irecord-uat.erecording.com/irecord_service/DataService/iRecordDataService.asmx	0%	Avira URL Cloud	safe	
http://https://irecord-dev.erecording.com/irecord_service/DataService/iRecordDataService.asmx	0%	Avira URL Cloud	safe	
http://10.98.134.15/isubmitservice/isubmit.asmx	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/iRecord.Common.DTOsI	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/IsValidFileTypeT	0%	Avira URL Cloud	safe	
http://www.gemedicalsystems.com/it_solutions/orthoview/2.1	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/MigrateOrganizationConfigurationsT	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/IsValidFileTypeResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/MigrateOrganizationConfigurationsResponse	0%	Avira URL Cloud	safe	
http://https://apps.erecording.com/Portal	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/InsertOrUpdateDemoXmlT	0%	Avira URL Cloud	safe	
http://172.17.3.125/DocConverter/DocConverter.svc	0%	Avira URL Cloud	safe	
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.SynchData/Service.asmx/	0%	Avira URL Cloud	safe	
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.ProcessInstrument/Service.asmx	0%	Avira URL Cloud	safe	
http://foo/usercontrols/usercontrol_password.xaml	0%	Avira URL Cloud	safe	
http://https://irecord-uat.erecording.com/irecord_service/ConfigurationService/ConfigurationWebService.svc	0%	Avira URL Cloud	safe	
http://defaultcontainer/iRecord_WPF;component/usercontrols/usercontrol_password.xaml	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetNextTransactionIDT	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetNextePrepareIDResponse#	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetNextTransactionIDResponse	0%	Avira URL Cloud	safe	
http://foo/bar/usercontrols/usercontrol_password.baml	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetDemoXmlT	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/CopyOrganizationConfigurationsEnvToEnvResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetNextePrepareIDResponse	0%	Avira URL Cloud	safe	
http://www.countyaccess.com/ROD_WebServices/ROD.WebService.SynchData/Service.asmx	0%	Avira URL Cloud	safe	
http://www.w3.o	0%	URL Reputation	safe	
http://tempuri.org/IConfigurationWebService/GetNextePrepareIDT	0%	Avira URL Cloud	safe	
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.ProcessInstrument/Service.asmxT	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/CopyOrganizationConfigurationsEnvToEnvT	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/iRecord_Server	0%	Avira URL Cloud	safe	
http://https://irecord-dev.erecording.com/irecord_service/SignatureService/SignatureService.svc	0%	Avira URL Cloud	safe	
http://https://irecord-uat.erecording.com/irecord_service/SignatureService/SignatureService.svc	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://irecord-dev.erecording.com/irecord_service/ConfigurationService/ConfigurationWebService.svc	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/InsertOrUpdateDemoXmlResponse	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/iRecord.Common.DTOs	0%	Avira URL Cloud	safe	
http://www.gemedicalsystems.com/it_solutions/bamwallthickness/1.0	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/iRecord_Server.ConfigurationServicec	0%	Avira URL Cloud	safe	
http://www.countyaccess.com/ROD_WebServices/ROD.WebService.ProcessInstrument/Service.asmx	0%	Avira URL Cloud	safe	
http://https://apps.erecording.com/Portal#Reports/Main.xaml	0%	Avira URL Cloud	safe	
http://tempuri.org/IConfigurationWebService/GetConnectorTransactionXmlByCountyGuidAndErIDResponse	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vip1.g5.cachefly.net	205.234.175.175	true	false		high
ocp.cscglobal.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ocp.cscglobal.com/cdn/gateway/csc/csc-logo-erecording.png	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://irecord.ingeo.com/SendOnboardingEmailT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://www.ingeo.com/AvailableCommandsT	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp	false		high
http://https://irecord.ingeo.com/irecord_service/SignatureService/SignatureService.svc	iRecord_WPF.exe.config.1.dr	false		high
http://irecord.ingeo.com/LoginT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://icongal.com/	iRecord_WPF.exe, 00000011.00000000.36262 4464.00000000008EF000.00000002.00000001. 01000000.00000005.sdmp	false		high
http://www.gemedicalsystems.com/it_solutions/rad_pacs/	GdPicture.NET.12.image.gdimgplug.dll.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/Y	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://tempuri.org/IConfigurationWebService/GetConnectorTransactionXmlByCountyGuidAndErIDT	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ocp.cscglobal.com/cdn/gateway/csc/csc-white-logo.png	iRecord_WPF.exe, iRecord_WPF.exe, 000000 11.00000002.531759467.0000000000812000.0 0000002.00000001.01000000.00000005.sdmp	false		high
http://tempuri.org/IConfigurationWebService/GetDemoXmlResponse	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.SynchData/Service.asmx	iRecord_WPF.exe, iRecord_WPF.exe, 000000 11.00000002.531759467.0000000000812000.0 0000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://irecord-uat.erecording.com/irecord_service/DataService/iRecordDataService.asmx	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://irecord-dev.erecording.com/irecord_service/DataService/iRecordDataService.asmx	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown

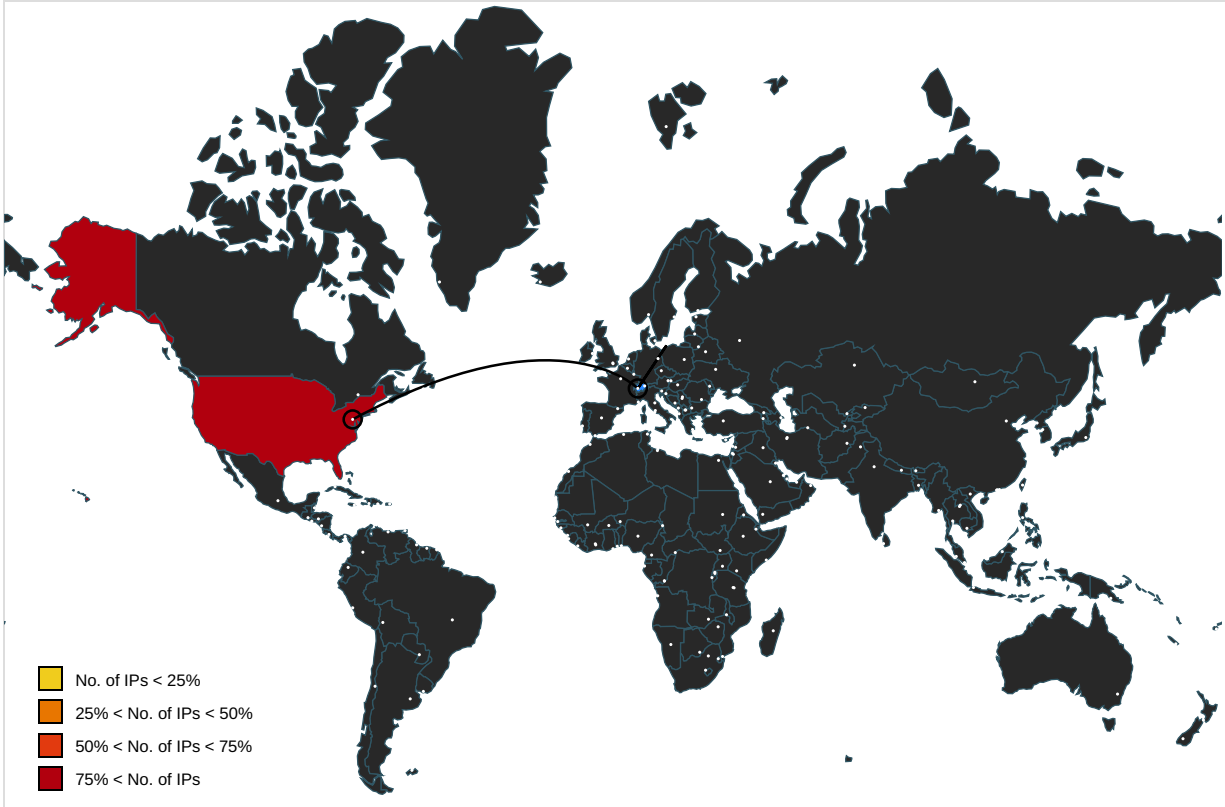
Name	Source	Malicious	Antivirus Detection	Reputation
http://10.98.134.15/isubmitservice/isubmit.asmx	iRecord_WPF.exe, 00000011.00000002.53581 8042.00000000031C1000.00000004.00000800. 00020000.00000000.sdmp, iRecord_WPF.exe. config.1.dr	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/SendForgotPasswordEmailT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http:// https://irecordbeta.ingeo.com/irecord_service/DataServ ice/iRecordDataService.asmx	iRecord_WPF.exe.config.1.dr	false		high
http:// schemas.datacontract.org/2004/07/iRecord.Common. DTOsI	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ingeo.com/TU	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord_WPF.exe, 00000011.00000002.536937886.00000000059 F2000.00000002.00000001.01000000.0000000 8.sdmp, iRecord.Common.dll.1.dr	false		high
http://irecord.ingeo.com/Q	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://irecord.ingeo.com/SendEmailT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://irecord.ingeo.com/T	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http:// tempuri.org/IConfigurationWebService/IsValidFileTypeT	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ocp.cscglobal.com/cdn/gateway/csc/logo-csc-ingeo.png	iRecord_WPF.exe, iRecord_WPF.exe, 000000 11.00000002.531759467.0000000000812000.0 0000002.00000001.01000000.00000005.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	iRecord_WPF.exe, 00000011.00000002.53581 8042.00000000031C1000.00000004.00000800. 00020000.00000000.sdmp	false		high
http:// www.gemedicalsystems.com/it_solutions/orthoview/2.1	GdPicture.NET.12.image.gdimgplug.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xceed.com/wpf/xaml/datagrid	Xceed.Wpf.DataGrid.dll.1.dr	false		high
http://irecord.ingeo.com/ValidateSessionGuidT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http:// https://ocp.cscglobal.com/cdn/gateway/csc/favicon.ico	iRecord_WPF.exe, iRecord_WPF.exe, 000000 11.00000002.531759467.0000000000812000.0 0000002.00000001.01000000.00000005.sdmp	false		high
http:// https://irecord.ingeo.com/irecord_service/iSubmitService/iSubmit.asmx	iRecord_WPF.exe.config.1.dr	false		high
http:// tempuri.org/IConfigurationWebService/MigrateOrganizationConfigurationsT	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http:// irecord.ingeo.com/SendTrusteeServicesNotificationEmailT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http:// tempuri.org/IConfigurationWebService/IsValidFileTypeResponse	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://irecord.ingeo.com/irecord_service/ConfigurationService/ConfigurationWebService.svc	iRecord_WPF.exe.config.1.dr	false		high
http:// tempuri.org/IConfigurationWebService/MigrateOrganizationConfigurationsResponse	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http:// https://irecord.ingeo.com/landing/assets/downloads	iRecord_WPF.exe, 00000011.00000002.53581 8042.00000000031C1000.00000004.00000800. 00020000.00000000.sdmp, iRecord_WPF.exe. config.1.dr	false		high
http:// https://irecord.ingeo.com/irecord_service/isubmitservice/isubmit.asmx	iRecord_WPF.exe, iRecord_WPF.exe, 000000 11.00000002.536937886.00000000059F2000.0 0000002.00000001.01000000.00000008.sdmp, iRecord.Common.dll.1.dr	false		high
http://https://ocp.cscglobal.com/	iRecord_WPF.exe, 00000011.00000002.53732 8306.00000000069F6000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://apps.erecording.com/Portal	iRecord_WPF.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://irecord.ingeo.com/irecord_service/DataService/iRecordDataService.asmx	iRecord_WPF.exe.config.1.dr	false		high
http://https://ocp.cscglobal.com/cdn/gateway/csc/ere-solutions-375.png	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false		high
http://tempuri.org/IConfigurationWebService/InsertOrUpdateDemoXmlT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://irecordbeta.ingeo.com/irecord_service/SignatureService/SignatureService.svc	iRecord_WPF.exe.config.1.dr	false		high
http://172.17.3.125/DocConverter/DocConverter.svc	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ocp.cscglobal.com/cdn/gateway/csc/csc-logo-erecording.pngXUa	iRecord_WPF.exe, 00000011.00000002.535818042.00000000031C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.SynchData/Service.asmx/	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/GetUserFromSessionT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://schemas.xceed.com/wpf/xaml/avalondock	iRecord_WPF.exe, 00000011.00000000.364624464.00000000008EF000.00000002.00000001.01000000.00000005.sdmp	false		high
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.ProcessInstrument/Service.asmx	iRecord_WPF.exe, iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/DeleteSessionT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://foo/usercontrols/usercontrol_password.xaml	iRecord_WPF.exe, 00000011.00000002.535635561.000000000335D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://irecord.ingeo.com/LoginWithDuoT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://https://irecord-uat.erecording.com/irecord_service/ConfigurationService/ConfigurationWebService.svc	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/IsUserUniqueT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://defaultcontainer/iRecord_WPF;component/usercontrols/usercontrol_password.xaml	iRecord_WPF.exe, 00000011.00000002.535635561.000000000335D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.ingeo.com/CommandT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false		high
http://irecord.ingeo.com/UpdatePasswordT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://www.ingeo.com/T	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp, iRecord.Common.dll.1.dr	false		high
http://tempuri.org/IConfigurationWebService/GetNextTransactionIDT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IConfigurationWebService/GetNextePrepareIDResponse#	iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xceed.com/wpf/xaml/toolkit	iRecord_WPF.exe, 00000011.00000000.364624464.00000000008EF000.00000002.00000001.01000000.00000005.sdmp, iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false		high
http://tempuri.org/IConfigurationWebService/GetNextTransactionIDResponse	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.ingeo.com/2001/v2/documents	iRecord_WPF.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://foo/bar/usercontrols/usercontrol_password.baml	iRecord_WPF.exe, 00000011.00000002.536355561.000000000335D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://tempuri.org/IConfigurationWebService/GetDemoXmlT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://irecordbeta.ingeo.com/irecord_service/ConfigurationService/ConfigurationWebService.svc	iRecord_WPF.exe.config.1.dr	false		high
http://tempuri.org/IConfigurationWebService/CopyOrganizationConfigurationsEnvToEnvResponse	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.ingeo.com/#	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false		high
http://irecord.ingeo.com/GetLatestVersionT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://tempuri.org/IConfigurationWebService/GetNextePrepareIDResponse	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.countyaccess.com/ROD_WebServices/ROD.WebService.SynchData/Service.asmx	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3.o	iRecord_WPF.exe	false	• URL Reputation: safe	unknown
http://www.fonts.com	iRecord_WPF.exe, 00000011.00000002.537791869.0000000008DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ingeo.com/)	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp, iRecord.Common.dll.1.dr	false		high
http://tempuri.org/IConfigurationWebService/GetNextePrepareIDT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ic-secure.com/ROD_WebServices/ROD.WebService.ProcessInstrument/Service.asmxT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IConfigurationWebService/CopyOrganizationConfigurationsEnvToEnvT	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/UnimpersonateUserT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://schemas.datacontract.org/2004/07/iRecord_Server	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://irecord-dev.erecording.com/irecord_service/SignatureService/SignatureService.svc	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.ingeo.com/Command	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp, iRecord.Common.dll.1.dr	false		high
http://https://irecord.ingeo.com/irecord_service/isubmitservice/isubmit.asmxYE-a	iRecord.Common.dll.1.dr	false		high
http://irecord.ingeo.com/ValidateResetGuidT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://irecord.ingeo.com/PushStatusT	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high
http://www.ingeo.com/SendEmail	iRecord_WPF.exe, 00000011.00000002.531759467.0000000000812000.00000002.00000001.01000000.00000005.sdmp, iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp, iRecord.Common.dll.1.dr	false		high
http://https://irecord-uat.erecording.com/irecord_service/SignatureService/SignatureService.svc	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/-	iRecord_WPF.exe, 00000011.00000002.536937886.00000000059F2000.00000002.00000001.01000000.00000008.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://irecord-dev.erecording.com/irecord_service/ConfigurationService/ConfigurationWebService.svc	iRecord_WPF.exe.config.1.dr	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IConfigurationWebService/InsertOrUpdateDemoXmlResponse	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/SendEmailAboutUpdatedEmailT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://schemas.datacontract.org/2004/07/iRecord.Common.DTOs	iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.ingeo.com/c	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp	false		high
http://www.gemedicalsystems.com/it_solutions/bamwallthickness/1.0	GdPicture.NET.12.image.gdimgplug.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://irecord.ingeo.com/UpdateAttachmentImagesT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://schemas.datacontract.org/2004/07/iRecord_Server.ConfigurationServicec	iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.countyaccess.com/ROD_WebServices/ROD.WebService.ProcessInstrument/Service.asmx	iRecord_WPF.exe, iRecord_WPF.exe, 000000 11.00000002.531759467.0000000000812000.0 0000002.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://apps.erecording.com/Portal#Reports/Main.xaml	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ingeo.com/AvailableCommands	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord_WPF.exe, 00000011.00000002.536937886.00000000059 F2000.00000002.00000001.01000000.0000000 8.sdmp, iRecord.Common.dll.1.dr	false		high
http://irecord.ingeo.com/ImpersonateUserT	iRecord_WPF.exe, 00000011.00000002.53693 7886.00000000059F2000.00000002.00000001. 01000000.00000008.sdmp	false		high
http://tempuri.org/IConfigurationWebService/GetConnectorTransactionXmlByCountyGuidAndErIDResponse	iRecord_WPF.exe, 00000011.00000002.53175 9467.0000000000812000.00000002.00000001. 01000000.00000005.sdmp, iRecord.Common.dll.1.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
205.234.175.175	vip1.g5.cachefly.net	United States		30081	CACHENETWORKSUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635361
Start date and time: 27/05/202220:17:52	2022-05-27 20:17:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RE_iRecord_Installer.msi
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean4.winMSI@6/73@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.3% (good quality ratio 33.3%) • Quality average: 87.5% • Quality standard deviation: 12.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target iRecord_WPF.exe, PID 7048 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\3e4f5b.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	18165
Entropy (8bit):	5.843732012251395
Encrypted:	false
SSDEEP:	192:sTARp3Nw/aJGPstaTARmxPPmcguW4EdcLDrvzWQCCNqyb/RT2loqI7PXKn8GS3Zm:skRgcqClQqQC6p2uqW
MD5:	BFFFB8526D93FFE19FFF51387F95E551
SHA1:	3BF7EE1BCDACC04A0B1F373364B88F0EF6716B3F
SHA-256:	B60F47D91C68D6953996300A163858F2BA229705A0680EE483075F6A27473A16
SHA-512:	EC9185363059647145001 3AEC3ED00A93A4B0657B9C9E7B4A6EE2C216CF02B40ED495B5755A0B15928D0E3C7713AB7A814A8E8F65651E6AB2171DCCEBEF4B7CA
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@k..T.@.....@.....@.....@.....@.....@.....&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}..iRecord..RE_iRecord_Installer.msi.@.....@.....@.....@.....iRecord.ico..&.{152FDDD3-47D2-4FCB-98AD-A21852A58929}.....@.....@.....@.....@.....@.....@.....@.....@.....iRecord.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{5E92A47E-6632-5D72-862B-8813B97D88D9}&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}.@.....&.{93D1A2DE-2F2A-5F74-9143-43A38E185206}&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}.@.....&.{6E797130-59F2-463A-85FE-097117D91A20}&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}.@.....&.{65238290-6439-43E6-981F-DDC4CD2EFD71}&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}.@.....&.{2C51C388-6C8D-4115-A9CE-23E781CF82F9}&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}.@.....&.{2C51C388-6C8D-4115-A9CE-23E781CF82F8}&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}.@.....&.{2C51C388-6C8D-4115-A9CE-23E781CF82F7}&.{FD00

C:\Users\user\AppData\Local\Programs\CSC\iRecord\BarcodeLib.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	113152
Entropy (8bit):	5.432506778804519
Encrypted:	false
SSDEEP:	3072:8vkiZ76ZyOnanSSbVmMPhPPmeuPeuUV9oLXvIUP/SqlPB5sqBTxvNeE3eezef3vW:88t0
MD5:	C00264CAA1CE15DD7295130C197C496C
SHA1:	BE413829FECE7461C196A473AED92340B5127CE5
SHA-256:	198DE06B2A96F2B7D889A24CF5E281783AF9E19D651BE39245EB35E8ED4DE88F

SHA-512:	AD9E6EBEB76C876CDBA9640544350E7E62D5CF8F59EC733665C2E77FA14A2EC96E13EABDD2B5B1385B451E8F17CCEDB55A41FE035249DA17FBD8F2ED9AA281D6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Z....." ..0....."... ....o... ..@.....O..... ....H.....text...(.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....0.....sd...}9....r...p}:....r...p};....r...p}<....(....}?....(....}@.... ,...}A.... ....}B....r...p}C....(....} D....r...p".. A.s....}E.....}F.....}H....(....*....0.....sd...}9....r...p}:....r...p};....r...p}<....(....}?....(....}@.... ,...}A.... ....}B....r...p}C....(....}D....r...p".. A.s....}E.....}F.....}H....(.....}:.. .*.0.....sd...}9....r...p}:....r...p};....r...p}<....(....}?....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\ClearScript.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	269824
Entropy (8bit):	6.02910870293459
Encrypted:	false
SSDEEP:	6144:tJ/jsB+ApSVX1VOSdFArxOmYF6JyICD08:Tb7X1VOSdFArAaq08
MD5:	0CAFBCA69177CEED3C71DF6E28F4EB4B
SHA1:	6A07E1B7BB4DA6754105255815DAC24A69ADFC47
SHA-256:	8E1F6224E34F9E4FEB61084913593F1828CB215104F102F816FCC4E7911796A5
SHA-512:	F09C1AF5211BB3DDF65720D89332F562193520C3E5EAEADD2949A7942AFBDC18E7CDD6D9939BD8CC3D555491C070717CC6C70B86E1DD19A3B2CE6D6DAD05E9F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K..T.....!.....5... ...@..... .....#G.. ..@.....5..S....@..H.....`.....`4..... ....H.....text..... ....`.rsrc...H....@.....@..@.rel oc.....`.....@..B.....5.....H.....]..p.....P .....h4..]N...9n[xM.6h..}...Ur##..5.....P.tK...Q..3.$.s`.....W..%eJ..+...C.....io.... .U..*.*.7.1P{...n..."u#.0..X.....(.....}.....s...}.....}.....}.....i....}.....+..{.....s.....X....i2.*6..u....(....*...0.....{....(.....{.....o.....{....(.....{.....+.....(.....X.....i2..{..... ....+.....o.....X.....i2...(....*...0.....-..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.barcode.1d.reader.64.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	512512
Entropy (8bit):	6.458327728775081
Encrypted:	false
SSDEEP:	12288:XL42VZeUqE0OQnvxQeHnPzZynNMh1gbXs7s9xu:b4KeUqRvxQeHnPzZynNMh1gTz
MD5:	827A493ACF99815266EAF004BCA62E63
SHA1:	ED0E915BEE644A600D50BFFE68DF9ACD090937FF
SHA-256:	8D651A792F64CD60EE1CF5EBCECB462FE28F5E90F743DF5005CD0F4F7ED4CC30
SHA-512:	B697920A6143773A8EA59C75B94C028A519C10AD41880055D5287C818FA64BF957B717D42EF48EE1E45B249CB1A343685E6AEE753223442A12A7226BF5F91A0D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t>`....t>b.G...t>c.....n..... .....Rich.....PE..d....G.W....." .....d.....0..... ..... K.....Q..<.....(.....V..... ..p.....p..... .....`.....text..... ..`.rdata...L.....N.....@..@.data....1...`.....N.....@....pdata...V.....X...f.....@..@.g fids.....@..@.rsrc...(.....@..@.reloc..p.... .....@..B..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.barcode.1d.reader.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	410624
Entropy (8bit):	6.6899628459906095
Encrypted:	false
SSDEEP:	6144:S2w7CVoglrCXkW1kzfaoR5/x1763q1rXCtY9HsS43oqG2EcWMPwUOoXT:SzCVoFkW1kmovwq1r4643oB2EcWzUDT

MD5:	109BFDD0EF4D12FD20DCF4E28C1F5AF7
SHA1:	71A50F51EDC181BB35CFD5504E458B551BEE6C02
SHA-256:	9A9B55E7AEAA574C21B07853236AA1A337545FCC688B0AE189C1EE29C5715ECE
SHA-512:	A27158817003044C1D6CEF362E419892A1BFDB2C19FC968AAFB669DFD23CDC102CC80D9E6387017A486FBBF38001D390C6A297F21D11C479A27FD05C2736E0E A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3[..`[..`.$.`L..`.$.`..`.$.`@..`8..aO..`8..aE..`8..aK..`R.e`^..`[. .`...`5..aU..`5..aZ..`5..`Z..`[.a`Z..`5..aZ..`Rich[..`.....PE..L....G.W.....!.....*...(.....c1.....@..... .....<....P..(..... .`...+.....p.....`...@.....@..l.....text...5(.....*..... ..`.rdata..J....@.....@..@.data....'.....@....gfids.....@..... .....@..@.rsrc...(....P.....@..@.reloc...+...`...,.....@..B.....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7639256
Entropy (8bit):	7.209210986696809
Encrypted:	false
SSDEEP:	196608:669HnDLeQDAvyCC2VWFJoDdLhlqBY4OPDq2sg:jLA4oDFhlqBYdsg
MD5:	72221A7EB81CE00918CFC4549219E411
SHA1:	6FDFC2B8440519C30AB48C1F7AF861814C3F6177
SHA-256:	C1827FB14D4F9E81C0177A84FBF49852EF6F7FB5A2D08FCFBAA8600C32AE5768
SHA-512:	82BC5AD6B20821D8CFA2E6856DB6A591147C970AF1F0CED6C57250E3A9822F578802D1465BE93519C96FF8535D3A89E99AB06D1E924D1628B905A5FCD5A927A A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'4.W.....!.....pt.....t.. ....t...@.. .....t.....,u. ..@.....t.W.....t.....zt.....t..... ....H.....text...$ot.. ...pt..... ..`.rsrc.....t.....rt.....@..@.relo c.....t.....xt.....@..B.....t.....H.....80.....9...:.....&.<.>."."..... 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ]..... .....h...(...t..... 0123456789abcdefghijklmnopqrstuvwxyz.....0...H...`...x...ED..rA..+N...K...U...P..._...Z...g...b...m...h..xv..Os...|..!y.....5.....[...l....%..? ..f/..Q*...4 ...1...>...;.....8...T...p..... ...<...X...t..... ...<...X.....|...X...B.....-...>...J...M....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.filters.64.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1031168
Entropy (8bit):	7.125043246657716
Encrypted:	false
SSDEEP:	24576:ZbxYDqMSpe3E0nBvQjdcCngvhiWaOuBuMgvhiWaOuButgvhiWaOuButgvhiWaOu2:ZX078gvhiWaOuBuMgvhiWaOuButgvhiq
MD5:	7F07C8D16F37EB5A2D3D1A12A2D53CAC
SHA1:	F69B30933555924A826334188D2AB05477CF32AD
SHA-256:	F468CAC8A1472117ABCE23DD275B6E0B1BDFABDE01F3D798F75833D98F6C7B5F
SHA-512:	A29306C404DB34C273E9813C4639634A230802965863BF7954B6B285B5376F1DF1D05B148F36359D4B7BF4BC7C7ED0B841550814F0BC3F0792735DDC3E18DFEE
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'...c...c...c....m.a...xd^.R...xd_.....xdk.r...j.f.d...c.....xdZ.....x dn.b...xdo.b...xdh.b...Richc.....PE..d....bW.....".....&.....4..... ....._....@.....<.....`...L.....0..... .....@.....text....%.....&..... ..`.rdata.....@.....*.....@..@.data...Pw.....T.....@....pdata...L...`...N..... ...@..@text...}.....^.....@.. data....0/.....0...v.....@..@.rsrc.....@..@.reloc..".....@..B.....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.filters.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	920576

Entropy (8bit):	7.2576447097984405
Encrypted:	false
SSDEEP:	24576:TjKrW8ungBY7y5b/963CwUK7bM7gvhiWaOuBuJgvhiWaOuButgvhiWaOuButgvh4:5ngBY7UrK7qgvhiWaOuBuJgvhiWaOuB1
MD5:	A4F761B3D974193CADF065FE2EE73D25
SHA1:	BF652BEA7F415A5E4F3D8D3CE3EB5F03367D317E
SHA-256:	44CBBA65C3AE910D14211FBF95239BBBA5D862C86647F7F274471D36D9BF25F5
SHA-512:	CC06226491A259EDED1DEB8C233BD7E7080E14F80B37943065431AF08181143F754907F8385A5F223BE188761F7695034A78C991C04633C96DEC160BC05A272C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f...".~.".~.".~.... .~.9;....~.9;....~.9;..~.+...%.~."...T.~.9;...~.9;. .#.~.9;..#.~.9;..#.~.Rich".~.....PE..L...E.bW.....!.....0.....F.....@.....P.....@.....`.....~..<..... ..|..... .....u..@.....@..\.....text..../.....0..... ..`.rdata..2Z...@...\...4.....@..@.data...Hg.....H.....@....rsrc.....@..@.relo c...,... .....@..B..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.image.gdimgplug.64.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	12596736
Entropy (8bit):	6.270521865379484
Encrypted:	false
SSDEEP:	98304:TUpCCZpTfuGmDb/ZMgvhiWaOuBuejgvhiWaOuBuguJuA6OojgvhiWaOuBuQgvhiG:YxiDbqbuJoOoAryvmKRS
MD5:	6291FD164861A1DAE116751845440117
SHA1:	32D55FD65D9FFB3F40B5E68E0A7782A9ED21E68E
SHA-256:	078D5ADC2900352B3632D18D77C0DC4CCE9E1CF9B6F30932EEA8DE0CBDB0AEAF
SHA-512:	F76A086347F2EB551384FCA7951B43A7300D7C0177E7379AFA0E5F1D36AC33B215BCABAE9AC81C5A2FB94DCF0E14B303DE75D59112629A2D28BB34144EB519 9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..._..._..._.n...._...._....._...^.}._..._..._.....L._....d._...._.... .._.....,....._.Rich.._.....PE..d.....W....." .....9.....b,.....@....."....@.....@.....<.....P..\..... .....9.....text...\.9.....9..... ..`.rdata...Ve...9..Xe...9.....@..@.data...p9.....I.....@....pdata..\....P.....h..... .@..@text....*.....,.....@.. data.....v... ...x...*.....@..@.rsrc.....@..@.reloc..d.....@..B..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.image.gdimgplug.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10847232
Entropy (8bit):	6.466938486708634
Encrypted:	false
SSDEEP:	98304:6wv53K1vgrjJPkxq5inR6mqITngvhiWaOuBuBjgvhiWaOuBuguJuA6OojgvhiWaw:6k5+vlj9gq5inRoIybuJoOoArJKzmK
MD5:	9D167ECA4FF3FAB92AEFBFFE7E0A00D3
SHA1:	84F51CEECD05CD2A5E96C18B4A16C0E7AEED9C2C
SHA-256:	A6F3F58BD894EDCE4DD495ACCA9183C2CDB132AA230EBC8D9A7FE24579D709B2
SHA-512:	E807FB4D48BA589F9BA062ED99029EC891B6BF6011CB6FE5B322D89EDC17B3BBEF423CF7E1D5E54AAE19EBFB1D0FAD7A85D48CB29696F1C905106855E645A 4C3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g..2#.za#.za#.za...a).zaL..a..za*..a&.za#.{a\.zaL..a..zaL..a.. zaL..a..zaL..a".zaL..a".zaL..a".zaRich#.za.....PE..L.....W.....!...../...u....kL%.....0.....p.....@.....P..;...t..<..... ....`%..@.....0.l.....text...../...../..... ..`.rdata....V...0...V.../.....@..@.data...X.....F.....@....rsrc.....,.....@ ..@.reloc..xN... ...P...4.....@..B..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.jbig2.encoder.64.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped

Size (bytes):	364032
Entropy (8bit):	6.473038675148677
Encrypted:	false
SSDEEP:	6144:Qe9Y2evHGeNHKXwsEOsSBPCU3muUpYJcTg3h8lKwswNF1kGdCiYeixHwqAE7i:j9Y2evJKXwsEshUpW8kGdCiYhQqAii
MD5:	C24214D16D48B53FBD5D4BC8B759CB84
SHA1:	81C97C1686A3C55A9A7997866532FF326D232BE1
SHA-256:	1D6B91172E65971A0439525BEFBE26497505F19965B8012187289EDDD0EFE4B0
SHA-512:	00CBE04291FB1B13C53DAA08AB603D673A890778A56E5D6108E52F0D2F3E9CCF6513B0266F49A6E966DE2E4A04473EF37777D8E6992887E74716E6F2376C8DE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...^.S.^.S.^.SI.PS.^.S..bS.^.S..VS.^.S..cS.^.S.&[S.^.S.^.S.^ .S..gS.^.S..SS.^.S..RS.^.S..US.^.SRich.^.S.....PE..d...x7`W....." ...../.....<.....P.....,4..... .....X.....text...Z..... ..`.rdata...C.....D.....@..@.data...Dn... ...J.....@....pdata..,4.....6 ...J.....@..@.rsrc...P.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\GdPicture.NET.12.jbig2.encoder.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	294912
Entropy (8bit):	6.613367101175881
Encrypted:	false
SSDEEP:	6144:Z/2zSZM42pHV+gVmEVYzInzojmT8P80GrYe/xCJ0:wWZNkVfmMzoiTl80GrYI6
MD5:	878061EB13201FDCB1FA83A5E770CE6C
SHA1:	DFB027D388277600698CEA600CF6CC42768D797B
SHA-256:	3CB4272DB5151F202C4AB1598CE9C3F06579C5A57A9F50A9E425B45580B95A48
SHA-512:	5A251C0B933F1683C1DCB5B49161BCD70FE258A2098061FAE38990EE9E0E0E5950BB0DF8E8665D5773B29B25E9A1DA94F4104C824F7A21528062DF1F6B8DCDE A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.L#+."p+."p+."p...p(."p0q.p.."p0q.p.."p0q.p.."p+.#pC."p"..p.. "p0q.p@."p0q.p*."p0q.p*."p0q.p*."pRich+."p.....PE..L...\7`W.....!.....G.....0.....@.....!../.....<.....P.....P..... .....@.....0.. .....text..... ..`.rdata.....0..... .....@..@.data...$b...0...D.....@....rsrc...P.....X..... ....@..@.reloc...!....."...^.....@..B..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Hexasoft.Zxcvbn.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	838144
Entropy (8bit):	4.710945748197975
Encrypted:	false
SSDEEP:	12288:TimqQPgH8T4J2+pWuyfPEWEmUVlH1beeb391Kl4Af7eOF:NqQPlT4JV6EDVb59a7
MD5:	73FB9E670EBFFC9664E30896936CCD54
SHA1:	15AACE485AFA741FC2490FA4A457FE18D7784A77
SHA-256:	12C019799E6A0305D2F93CBDC3FEA62FD00D662B4769EA180DF2F9C5F8377820
SHA-512:	C236B88BA1F2734BB8EA19D7D6862C176426FDDC9142969A096FC9B24CCBAFEB48CE8922A795B9E54D46689C0B8B1A9CDF6E6EC4E91F975BA9F90D1056DDC CA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....X....." ..0..... ....@..... ..`.....x...O..... ..... .....@..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....4.. "....V..p.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(.....(.....(.....(.....(....*..{....*"..}....*..{... .*"..}....*..{....*"..}....*..{....*"..}....*..(.....(.....(.....(.....(....*..{....*"..}....*..{....*"..}....*..(.....%-.&r...p(.....%-.&(...+(....*.0.....(....~...:....~....%-.&~.....2...s....%.....s.....(.... (....%o....o....r...p(....o.....s.....o....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Hexasoft.Zxcvbn.pdb

Process:	C:\Windows\System32\msiexec.exe
File Type:	MSVC program database ver 7.00, 512*59 bytes
Category:	dropped
Size (bytes):	30208
Entropy (8bit):	2.964751279521241
Encrypted:	false
SSDEEP:	192:zjAgAykAXnAjAm+DA+RxCIEYvVYHsOiKANw/dtJE0J8p5NL86syWasfGanJYmKnL:TDux+LCIRvVYR/V7C0KKPDXZn2fR7

MD5:	C6BEC72BDD322D03B65757D2F6014289
SHA1:	121975A4A4A7C54103626519126D29CAA323193F
SHA-256:	D877B97520860912D925C174E5B85C4E20A05673EF321714BC2DFA51E919D2E4
SHA-512:	C16A18826B1DF28364AEA5936DA4846E4C23261B8B4D5F3AFA2F3CBDC644BE150DE97AC9C1AF03F729BBBFBF60516AE3168BD2F727757547111F277B6B5501D0
Malicious:	false
Preview:	Microsoft C/C++ MSF 7.00...DS.....;...(.....7..... ....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\JavaScriptEngineSwitcher.Core.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	26112
Entropy (8bit):	5.354566580296006
Encrypted:	false
SSDEEP:	384:LtY3HKlv2uHfVhV/Yp8RZpfTd4KJzbGpE/M1z/SIZ+uK5pkgvsjozCBAJd:LtY3HKlv2uH5/df3JzbgEmbEp5CBGd
MD5:	798D5E3838A4607A413D1EDE6B6EE8AA
SHA1:	82254856680584024C89888E51FB9E3643F2DB6C
SHA-256:	0E5FEFC870E2F631ABABC823272A5C1C1ED129C6A493D8C34756FFB61FBF4905
SHA-512:	DA8DA019B2A2592B16FBB53F69E34A0B298627E159EF797C5EE22C37FE5E361A4B2F4FE80AAB63DB981BEC7671122F4078ACBEA3719A4B4BA10B277CC72DBE64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....-S.....!.....^.....}... ....-.. ..@.....P}..K.....\|..... ....H.....text....]... ...^..... ..`.rsrc.....`.....@..@.reloc..... .....d.....@..B.....}.....H.....@...<.....(2.....P .....Q.Mt.'.W..R..XU.I...}x...dYI..^...$..S\".De7o]....@.....1.}3.\...*c[@...0^...Shj...M.@..}..L.|.(wu...+..(.....F.r...p(....t"...*6.r...p.(....*F.r...p(....t....*..(....*F.r-..p(....t"...*6.r-..p.(....*F.r7..p(....t"...*6.r7..p.(....*..(....*.s....*2.t....o....*6..(....t....*..(....*"..(....*&...(....*..0..... ...s.....rA..p.....(z.....o.....(....&.o@...(....-%.rA..p.....(v...

C:\Users\user\AppData\Local\Programs\CSC\iRecord\JavaScriptEngineSwitcher.V8.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14336
Entropy (8bit):	5.3431585937255575
Encrypted:	false
SSDEEP:	192:Z5cYDhpOaFQHAQEeae/jGwnvGNVKk01GyUzbpBZsXVTRY8FeYJTsd5WaS4:IY1watQEeXSwvBypBZsFTRvebAu
MD5:	34D88D8ED60A7BC45DE2AE9126EC1E9A
SHA1:	0C6A4CF4FE26DAC6D862EDD41B9F776AF3464F9C
SHA-256:	6E72C948EE64BF8EAF850775440F03F8A2DFD4BE62BAAFA0EEE69D2F8ED5E49D
SHA-512:	7BF1B90FF2593F8062E4D840C037FD97009DE31C8373BCC52DED1EFCC6B176E200F807371CBFEFE7EFB9A847DE92485BA4A5535CA543F2F28BE12B6FDB1A74F9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....T.....!.....0.....NO... ...`..... ..... ..@.....N..O...`.....M..... ....H.....text...T/... ...0..... ..`.rsrc.....`.....2.....@..@.reloc.....6.....@..B.....0O.....H.....+.. ".....(.....P .....!.yoK...O*4v.(.#8..*..;T...-9C3.$[J.&Q+.n....n'.....H...RTi.q.}.\.T..U..O.. jC>....<.7.6.F.SL.N<.V9.&{}.i7'..~...,.. h\."[.^(.....s....o....*.0.....o....r...p.o....9.....t!....(....-.r...p+.r#..p..o....o.....(....,..o.....r)..p(.....rG..pr...p.(.....(.....(....-`(....,H(....o ...r_..po!.....r)..p(.....(....-.(.....("...s#...z...(.....+.(.....("...s#...z..($...-.(.....("...s%.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Microsoft.ReportViewer.Common.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	6391672
Entropy (8bit):	6.145134623846332
Encrypted:	false
SSDEEP:	49152:eLoY0vX6K4/vkJvFViWOEl6eM0bEmRR0eZhIne76WLN1ksrsDTjRDPlx61PL:WK6K4/m83DeM4seHwmL86UKD
MD5:	1AB118E292B518FCDBDB4E6DFFD6E859
SHA1:	264036E40BFA9FED82D67D2C9A7B9D0BE570CD3A
SHA-256:	E475122047A36371F61E86B8D099FC8D6F263BD3BDB03D00B1116B0CB5B28636
SHA-512:	572F52A294890AF88B860AB3887970C1268713D56AE3917E0865766D84B12FD1728688C5F2F931FC20FA88DD4A2BE0E1F70E7D06926E592687B4BF5ECA4095AD

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._M.....!.....fa.....a.. ....a..... .....a .....Mkb...@.....a.K.....a.....pa.x.....a.....a..... ....H.....text....ea.. ...fa..... ..`.rsrc.....a.....ha..... .@..@.reloc.....a.....na.....@..B.....a.....H.....1...0.....h.'.....P .....9.G..*.f=..g..2..8...].>.1q.....\..."..(q|.'o?..Z.C**.....Y....7...?.sq..ofz .....-.~\.\a.(i..z..2..4 ..Ev...r.....R.Nj..(t.....}.....s....(u...*>...-..+..(v...*..0..%.....Q.{.....(w....(....,..*....sx.....(y.....;....8.....{....-..s....}.....(z...u.....,..o{....(.....(|...-l.,W..o}.../Nr.. .p.o~....(....,;.o}...s.....r!..p.(....o.....r9..p.o.....{.....o....&8.....{.....o....&8....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Microsoft.ReportViewer.DataVisualization.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3875728
Entropy (8bit):	5.956619608882082
Encrypted:	false
SSDEEP:	49152:YxdSUT1d9eFT381NfA+XvtnLNkxSYSMdqD990V62E/vWCU:q8b36Pkrjt
MD5:	6A3BCCCBF8D945A666D825B85D6284F0
SHA1:	B59032024D576446AFAA7565F68883D915FEB731
SHA-256:	6ABB0C733248C3CAE99C58512A6E2B4F938FAD3420203E96EB03C9CB1AAB60B7
SHA-512:	6A2B4E853384F603790E3F109808C6F69433F49E38242A1E01C76BB0F10145EF76833D39EEE91E56B9788B8D57EDC8CDBED63A19813A083751677C2ECE62EAC3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._M.....!.....;..... ;.. ...@;..... .....;.....;. ..@.....D ;.W....@;. .....;.....`;.....;..... ..... ..H.....text....;.. ....;..... ..`.rsrc... ....@;.....;.....@..@.rel oc.....`;.....;.....@..B..... ;....H.....!..x.....0.....P .....hlO. 5...5zBj.gM+..o(.&...vB7z.Q.c6.@)o..&9.SU3.oi.[.n_.S..@hd...r4.R$R...3. ,.\.+C*.C..T.....(W.....D../...)..~.B..(...*.(h...*..(i...*.r...p(j...*.rE..p(j...*.r...p(j...*.r...p(j...*.r%..p(j...*.rq..p(j...*.r...p(j...*.r...p(j...*.rQ..p(j...*.r...p(j...*.r...p(j...*.rE..p(j...*.r...p(j... *.r...p(j...*.rK..p(j...*.r...p(j...*.r...p(j...*.rG..p(j...*.r...p(j...*.r...p(j...*.r3..p(j...*.r{..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Microsoft.ReportViewer.ProcessingObjectModel.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	92056
Entropy (8bit):	6.034556170881513
Encrypted:	false
SSDEEP:	1536:im+rBQpJ7dJg+wqtetLRBQi+IYKDjrMr9Yqds4JUQ9rHUgP:p0B+JRSBqtS9Bm9Uq2CUQ9o4
MD5:	C6021782BFFBE07C8D79A4171A55F36F
SHA1:	1BA19B627901BE3C895C089397EE4DB86C27B6EC
SHA-256:	68DF6E12892CDD9244D50BE4C0BAA22A9E14BBA4E64655521B29C17EBAED2A24
SHA-512:	F0914B903ED79B3EEA270CD89F770FA0BA647C931E91CA57FEBF7C12CA44F2ACFE8C08A2C018A7630126EFF02381DC965A9E95E2AAE2470208FA8B10891C7A 96
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._M.....!.....F.....e... ....@.....d..W.....@.....P.....d..... ....H.....text....E... ...F..... ..`.rsrc...@.....H.....@..@.rel oc.....N.....@..B.....d.....H.....;..X(.....P .....U.J./Xvf..4...{h...Q.d.. _..b.vj..>.Jd_B.h..u...P..H~....N.....z...#.V.+q.....>G ..=..f.sU... z/@UN<.A*xibE.^@<.c..:.(.....}....*..{....*.*..o....*".}....*2.{....oM...*2.{....oN...*2.{....oO...*2.{....oP...*2.{....oQ...*2.{....oR...*2.{....oS...*2.{....oT...*6.{.....oU...*6.{... ..oV...*6.{.....oV...*..(....*..(....*..(....*..(....*..*..(....*..*..(....*:.(.....}....*.s....z.s....z6.{.....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Microsoft.ReportViewer.WebForms.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2136960
Entropy (8bit):	7.283824146891077
Encrypted:	false
SSDEEP:	49152:NgJUzOAMMfsbDjIFZOzQYtpf5sZ0RIgF4xD151bzoA0y0oDJe6gD/Q1IjQj0jytA:mJr04SQqqCx
MD5:	E337CA3F8AE598D3065C932E4186B0A1
SHA1:	C39533068318BFCFC05D5F05C9E799C01013F13F
SHA-256:	6B488659B937014469CF01973F0055B0C817FB6A15D0F136C0FB405B2E4524EC
SHA-512:	EF7DA045A11F4E9FB7E1709CA693B0271753CD0471A8C3FF331CF28590687DBD7F17F2F213A9DDEBF6EE0EA8D06302E7DF33F6FDB263B9F60CFB86861428B7 6
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._M.....!.....z .....N. .. ..].!. ..@..... .O.... ....\. ....H.....text...Ty .. ...z ....`.rsrc..... .....| .....@..@.reloc..... ....@..B.....0. .....H.....f...1.....0.....P .....\_.+.:I..... .\a.....&..Q..D/.X..?..."@.x....*.4.....qpZt.J,..y.@..g.6....m*;.....t...'.3.WS.....(. [>..|...,.rs.G..%..|'4z....($...*..($...*..{B...*.0..e.....}B....r...po%.....(&...,..r...po%.....(&...-....(....}(....((...o%.....,..t....r7..p.o'...,...}6....{(...,`.rl..po%.....(&...-L..o.....}+.....r[..p((... .....o)...r_..prc..po*...(+...%..},.....}1....re..po%.....(&...-...}%....r{..po%....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Microsoft.ReportViewer.WebForms.xml

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	135305
Entropy (8bit):	4.921878220786072
Encrypted:	false
SSDEEP:	1536:nfKXiU5vym2ILot73P9XfiYfipfibiFitisasBt7D0rcCJEyiti+i5iOZib:nfKXiEct73czom4gsasBkcCJE5g18v
MD5:	D09AF9238DC6F9107EAE65166AD12F04
SHA1:	F3B3824D9091D913653FBA694E23A4B40FC4EA0B
SHA-256:	2A4BE0909FF0F4D276EE7866E5FE0ABC50D56A40C80195C0C8AB511C179F00BF
SHA-512:	F6C6D65B06B27D3AD0CBAE34A8A4E18D458B55EB568E7D74DD1D86535680A5C47D0253BCB9A25FEDA7C97D6C5667F4D95E1C731C4BCFB999D9FF24F9FDC2 0A8
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<doc>...<assembly>....<name>Microsoft.ReportViewer.WebForms</name>...</assembly>...<members>....<member name= "N:Microsoft.Reporting.WebForms">.....<summary>The <see cref="N:Microsoft.Reporting.WebForms" /> namespace contains methods and properties for the Rep ortViewer Web server control.</summary>....</member>....<member name="T:Microsoft.Reporting.WebForms.AspNetSessionExpiredException">.....<summary>Occurs when the ASP.NET session has expired.</summary>....</member>....<member name="T:Microsoft.Reporting.WebForms.BackEventArgs">.....<summary>Provides data for the <see cref="E:Microsoft.Reporting.WebForms.ReportViewer.Back" /> event.</summary>....</member>....<member name="M:Microsoft.Reporting.WebForms.BackE ventArgs.#ctor(Microsoft.Reporting.WebForms.Report)">.....<summary>Initializes a new instance of the <see cref="T:Microsoft.Reporting.WebForms.BackEventArgs" /> class. </summary>.....<param name="parentReport">The parent report of the dri

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Microsoft.ReportViewer.WinForms.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	548224
Entropy (8bit):	5.999516972643781
Encrypted:	false
SSDEEP:	6144:ZjRzVOuWKe7M2+HEEZ0yZ94D6q/oNWW5B/PrKKGXHMBagTFGID0dBOWfQP752+VC:HVO7nrwBx5hGj/8651
MD5:	9009C3B320D67C0972BB8CF542D9078F
SHA1:	E45E9A4F4DDE77613A882E6BEC1906C084656DF2
SHA-256:	EACC72C00295D057C3AD9AAAAABEF3086CA52A14FA717E16EF05340011A71F88
SHA-512:	54B9CBB041DD455CA238E2A2277E5CF237FA9F87B928A05B6BE7FA212C047BD0B7B92533AF3A46B7C4E5FC6ECDA5EAFF054CC281DA90E344E9782918A55D65 D6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._M.....!.....<.....Z... ...`..... .....d... ..@.....4Z..W...`.....F.....Y..... ....H.....text...`:.. ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....D.....@..B.....pZ.....H.....h...,.....Q...6..P .....l...u..QP.S-.j....w_...F. ...L.)..P.....4.....s.9.....:.>x...g.v2P..o`.~k..-... ...0=....*o...../3...+D.....|..r...p}.....}.....s!...}.....(!...*..{....*"..}....*...0.....o....*&...(....*..0.....(....*..0.....o....*6..o....o%...**.(.....*..{....*"..}....*....0..... ..(.....&.....*.....0..1.....{....%.("....o....,..o!....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\ScintillaNET FindReplaceDialog.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	83456
Entropy (8bit):	5.448697019029869
Encrypted:	false
SSDEEP:	1536:xw37VrvesHwmluCn0HF8Iwby6FT4xJKd7BD0sYlMT8+8hVg72BnFs:wSwbyxJKd7BD25+8ZnFs
MD5:	BAAD629D739A8437ADF66B2D5B2BFC52
SHA1:	EC3AB2B8A3697FD1FDF962FF466B734CAF020A8B
SHA-256:	42B0BEF1D60015D26AF76A13E83B1D77707789DDCE6C8233AD7E13B1EFD562C3
SHA-512:	1CBA882D906702FEB1CAFA1C28A3BF2EA2B8E7D75ADB9F51D5DBD0D7841480DFA3B0B3307D223C2E72EB492592D6ACECB8E46900F5C64B1A811F311CA4601 020
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y=.X....." ..0..<.....[... ...`..... ..... ..@..... H[..O...`..4.....Z..... ....H.....text...;... ...<..... ..`.rsrc...4....`.....>.....@..@.reloc.....D.....@..B.....\|[.....H.....G.....>..}.....}....*..r...p}.....(.....oW...}.....,...(....*"..(....*...0..).....{.....(....t.....\|.....(...+...3.*....0..).....{.....(....t.....\|.....(...+...3.*....0..).....{.....(....t.....\|.....(...+...3.*..{....*....0.....}.....{....o.....o....}.....{.....o.....{.. ..(....o ....{....(!...o".....{....o#.....o$...}.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\ScintillaNET.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1368064
Entropy (8bit):	7.925726997854763
Encrypted:	false
SSDEEP:	24576:IJSShz305vgNF7/cOCPHPSVs4Eq+QTNX+cfQdS+2MMPishd/Ws5:ti0aNvoHqs4L95X+cfx/HGC
MD5:	9166536C31F4E725E6BEFE85E2889A4B
SHA1:	F0CD8253B7E64157D39A8DC5FEB8CF7BDA7E8DAE
SHA-256:	AD0CC5A4D4A6AAE06EE360339C851892B74B8A275CE89C1B48185672179F3163
SHA-512:	113A7B77D2D557D135470787DEEAD744D42F8292D853E2B55074E9CB3591FD045FFD10E5C81B5C15DDE55861B806363568611E591AE25DCB31CF011DA7E7256
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4.X....." ..0....."... ....@..... .@.....O.....P..... ....H.....text...(... ....`.rsrc...P.....@..@.reloc..... . .....@..B.....H.....<....%....."..(3...*....0..q.....,d.o4.....(5.....(6.....,L.s7.....+7...o8....m...,"....r...p(9...,.....s\...o:. ..&...X.....i2..*....(;...*6.,..*..(<...*..*..{....*"..}....*..{....*"..}....*..|....(=...-!..{....ob....{....o....s>...}.....|....(?...*..0..D.....{....-5..+...X..{....(@....XG-...{.....{....o9...(E...}.....{....*..(A.....}. .....}.....}.....(.....(....*..{....*"..}....*..{....*"..}....*.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\ScintillaNET.xml

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	416991
Entropy (8bit):	4.460121829044502
Encrypted:	false
SSDEEP:	3072:68mrJTCSI3h8A7og8PNmiFdhvuiUbOtYo96WYpIJ/ZdUu0e4Yc+IAVU:6NXWoYAVU
MD5:	E200C312A4C43F78021A9CFD75B0B9D2
SHA1:	27399C877E289167B715C727A97CB6DB26108DDA
SHA-256:	D40A05B1D45B13C7AD7395024743E68667A340D488CD9ACD71BC4824D6944538
SHA-512:	3BAD4F3085C5C2C3608BCE8FEA7C83BF063E579ACDBDB2CB277036FB17328573E02936C9B23A17C3EB04CDFFBE3441D358D141930C3E1A7654D22E2800BA3 EA
Malicious:	false
Preview:	<?xml version="1.0"?>..<doc>.. <assembly>.. <name>ScintillaNET</name>.. </assembly>.. <members>.. <member name="T:ScintillaNET.Annotation">.. <summary>.. Visibility and location of annotations in a <see cref="T:ScintillaNET.Scintilla" /> control.. </summary>.. </member>.. <member name="F:ScintillaNET.Annotation.Hidden">.. <summary>.. Annotations are not displayed. This is the default... </summary>.. </member>.. <member name="F:ScintillaNET.Annotation.Standard">.. <summary>.. Annotations are drawn left justified with no adornment... </summary>.. </member>.. <member name="F:ScintillaNET.Annotation.Boxed">.. <summary>.. Annotations are indented to match the text and are surrounded by a box... </summary>.. </member>.. <member name="F:ScintillaNET.Annotation.Indented">.. <

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Signature.XmlSerializers.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	4.780501953683461
Encrypted:	false
SSDEEP:	192:kHGGJFyic6RMQ9szqq2v3P+G+Am6PsFasJEQJKU4sI:kHGGJkwM7qq2v3P+G+ysFbEgKU4sI
MD5:	5215D1E404057E12C8006030A9C7F394
SHA1:	120A26901A51801BE3113855778A46D37D90409D
SHA-256:	8780FBC4F998243B17C3DC84F8F0E462C9E02053B984A6E49BFAEE1A90A81408
SHA-512:	E31F4128AB98A254317791A99222ED5473D15FDF0C84199B3DE0174F00A17A523B1B63B0BA7721B68F2E916ADE2A854EA7FC761BEF7B6D9FAB36BB5F4141809 E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$..\.....!.....&.....D... ...`..... ..... ..@..... C..W....`..... ....H.....text....$... ...&..... ..`.rsrc.....`.....(.....@..@.reloc.....,.....@..B.....C.....H.....+..... .....-..r...pr-..p(....*.(.....r...pr-..p.t.....(....*..(.....-..r/..pr-..p(....*.(.....r/..pr-..p.t..... (....*..(.....-..rS..pr-..p(....*.rS..pr-..p.....(....(....*.0.....E.....\"...*...2...:...B...+Hr_..p.+[ry..p.+Sr...p.+Kr...p.+Cr...p.+;r...p.+3r...p.++r...p.+#r5..p.+...j...(....(....rA..p(.. ..z.*....0.....-...,....(....*..-!.o.....(....(....-...(....z.....(

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Signature.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.988467876256735
Encrypted:	false
SSDEEP:	192:R/FoVSxYTCWElOeV4DMbVyeHx/3G7xESHXvftaHt4LeyWrZ:V2VBCWEVV4r+3CXVlyWrZ
MD5:	ED0C7D9AE402EC07A2476E5B3F64F686
SHA1:	862AD4DE22FD86588FF3FE0010B320E8FEBF8FFA
SHA-256:	2FE8EB90D42B0C47F8A506A6960FD2F9645365C00C4151EBA6E0073FAFF6D94B
SHA-512:	DB34F36B1B6EB58455D30E6D4033CD812B71AF355C7D21783AE3DF910B2F836C4D11365357D5A491362B241A66754F82CCC9E3A2842383055361EEEF1264212F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..\......" ..0..(.....G... ...`..... ..... ..`.....`G..O...`.....(F..... ....H.....text....'... ...(..... ..`.rsrc.....`.....*.....@..@.reloc..... .....@..B.....G.....H.....&..X.....Jr...p..(....(....*^s....%s....o.....o....*..(....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*0..A.....(.....%.....o....(.....(....(.....(.....(.....(....*Fs.....o. ...u....*..0..4.....s.....s....%s....o.....o

C:\Users\user\AppData\Local\Programs\CSC\iRecord\System.Net.Http.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	6.047144934824472
Encrypted:	false
SSDEEP:	768:owZsX9msB1fSbljwY3qbvgk/6GvrNn//Hsqzd2pwmk6Iq8QOMcym5iiou3Lm:aNmgZSpeRJ/Hsyd2bTWMcT5qu3q
MD5:	0EC477E70D36FB89CFEDB1921D36A1EB
SHA1:	ED8352CBCED9E1AEAF958195E7F5F92C5ECE5ACF
SHA-256:	A7AA24413BCB339854708865A789A8860CF04392886CD7B981A916CCB6CCD5FF
SHA-512:	967FCE0B8FA932632460982406F44E1806906EF7D5EA4AFEE528AEDDA538189BA3A9B3069DB57694DBEE0798C301EB19DD8C9D168B389B0F3E68C0FB3B4BE2 8A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....bP....." .....^.... ... .a. .....`..... ..`.....O.... ..T.....>...@..... ....H.....text...d.... ....`.rsrc...T.... .....@..@.rel oc.....@.....@..B.....@.....H.....#..x..... ....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\System.Windows.Controls.DataVisualization.Toolkit.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	351744
Entropy (8bit):	5.934530976323409
Encrypted:	false
SSDEEP:	6144:mqZ4qEuVEAPKOuS8EsbVq+gjdyGSm49YaU8GkwS9WK4U0VEcLjLU/mp0:mqZ4qEdOuS9sbVKKm2
MD5:	406C457D3D29E3091A8594BA086E6E82
SHA1:	56FE4D37FB6938A78F99E667ECA79F8D6BFD2DCA
SHA-256:	AA5732B41C0F633993BADF09AFCA15E0668BD888784CFEA1249FB4FFD6DA133D
SHA-512:	480D013C33AC8CCECC5A54BCF0EB06AE1BF910B5B269268B46FA1FA8720C9A1E397AE0C5BBCB6785CBA3562BE77115AB15969778D49D958C1272B64540FEA6 B8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....JUT.....!.....T.....nr... ....@.....r..W.....p..... ....H.....text...tR... ...T..... ..`.rsrc.....V.....@..@.rel oc.....\.....@..B.....Pr.....H..... \.....p.....(....*.0..4.....s.....o.....+..o.....(....&.o....-....,..o.....*.....).....{!...*"..}!...*... .0.....("....o#.....("....*.....n.($...-.(z...s%...z..(&...*r.($...-.(z...s%...z...('...*r.($...-.(z...s%...z...((...*j.($...-.(z...s%...z.()...*..(*...*..(+....s,...(-....(...../...s0...o1...*.. (2...*..(2...*..(2...*..(2...*b..{3...{4....{5...o6...*.0.....s7.....{8..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\System.Windows.Controls.DataVisualization.Toolkit.xml	
Process:	C:\Windows\System32\msiexec.exe

File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	630554
Entropy (8bit):	4.57251756614522
Encrypted:	false
SSDEEP:	1536:GD0sPITh2l1RBCTJWcSuJ0BdnJGVunAoI2uQK+xzVTVrlzMt/uGLvKcKpjDjM5wG:efnPBdx/qM+9IXG85jLXl0Rp
MD5:	6A9EE40E8C10F20ED2761C5BE130944E
SHA1:	CDC757F407BAA53B3E55B373B1B3A7F500B4130F
SHA-256:	4FA61A08DC7B5791400506D4F88AA72A1DCB6F0858CDC8DDC39F4E87BF861390
SHA-512:	503E98445A1F4F1AF472D0CB072D67B4E3EE0F8E116CE4C02BE58D416DB1C137EC96FD7741C750F933B5AAE4CA3194121C3235BDD980A7843220A4935D0E482D
Malicious:	false
Preview:	<?xml version="1.0"?>..<doc>.. <assembly>.. <name>System.Windows.Controls.DataVisualization.Toolkit</name>.. </assembly>.. <members>.. <member name="T:System.Windows.Controls.DataVisualization.AggregatedObservableCollection`1">.. <summary>.. Aggregated observable collection... </summary>.. <typeparam name="T">The type of the items in the observable collections... </typeparam>.. </member>.. <member name="T:System.Windows.Controls.DataVisualization.ReadOnlyObservableCollection`1">.. <summary>.. An observable collection that can only be written to by internal .. classes... </summary>.. <typeparam name="T">The type of object in the observable collection... </typeparam>.. </member>.. <member name="T:System.Windows.Controls.DataVisualization.NoResetObservableCollection`1">.. <summary>.. An observable

C:\Users\user\AppData\Local\Programs\CSC\iRecord\System.Windows.Controls.Input.Toolkit.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	109400
Entropy (8bit):	6.071956198915581
Encrypted:	false
SSDEEP:	3072:G+s08khkhGbYzCripb/8JExywW9lGW7MPSXfciFTd95:G308khN8IExyrSWGKv
MD5:	9722713E648F42B57299E9D2CF3D5C1A
SHA1:	A4D0DC4F09CE84A33F1AA3E0C5CB4AE131F9FB0C
SHA-256:	BC3A78EB4DF2FD5B39244FA0586CC0A82FE3D0E185D151E6C340C53072A61872
SHA-512:	F6BB5724DFC46476E94448ECB4650AD23197CA21965EDF923E5D8BF51A31A707C058BCA6CBAC8E40E324BB54944DA4129659DC2D2FC965E260BD40123A8AEEBB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....K.....!..... .....@.. .....~`... .@.....W.....0.....X..... ..... ..H.....text..... ..... ..`.rsrc...0.....@..@.relo c.....@..B.....H.....l.....0~..9<..P .....~.mM.z..L..#....K...L.eY$.....R.1.....wSn./.\fl.....h..../..U9..$$..... .....e. TY.y><".#/M.....".s!...*..{#...*"..}#...*..{$...*"..}$...*V.(%.....(&.....('...*F.~....(*....d...*J.~.....d...(+...*...0.....t.....o....*..(6...*..{....*"..}....*..{....*"..}....*F.~....(*....e...*J.~.....e... (+...*....0.....u.....(,....e.....o....*.0..m...../.(....s-...z.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\System.Windows.Controls.Layout.Toolkit.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	95064
Entropy (8bit):	6.069925755579635
Encrypted:	false
SSDEEP:	1536:ejt4SdWiPPH+PhqaEMN+3esQG0AZGblWfp8/x1il5OvNYXBTfciwN9rHUj:ejt1Yi8KUblWfpqwdXBfciwN9o
MD5:	22D9D032858972B8EE628FA818AB04DB
SHA1:	6EEAE133E394292C6C349F838114C2A39DFE8357
SHA-256:	E3D7F794442D9DBE99F5D578C0BC8D9E3198FE4055CF5581FC1DE78085967C50
SHA-512:	6899B2650AAFD1E88049303C7EE26FF7E0DFE201D8A7188386EF2354DEEB32F611BB4B73A02BE9127FC96D5B4D37CAB9BDBEC3CFCB3BF4CADA43170AC4349E0F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....K.....!.....R.....p... .....@.. .....0j... .@.....Pp..K.....8.....\..X.....o..... ....H.....text....P... ...R..... ..`.rsrc...8.....T.....@..@.relo c.....Z.....@..B.....p.....H.....L...`.....xr...I..P .....g.....o..g.Y...O.*....o.d....y.R2@...C.l0.HI..UV..U.(..K32[.`[@J&%~*&.;...+.n8 ...I[b.w.....KT.'y..j7=!p9R9<.u.....h."..(....*..{....*"..}....*..{....*"..}....*F.~....(.....Y...*...}.....~.....Y...(....}....*...0..-.....t.....{....-....(!....Y...o....(....s"...z*..{....*....0..F.....{.....{. .....s#...o$.....}.....{.....{.....s#...o%...*F.~....(....u]...*6.~.....(...*..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\WPFToolkit.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	467288

Entropy (8bit):	6.047761304423497
Encrypted:	false
SSDEEP:	6144:ABk34hZ9hNZbkDu0WtH7epyiNrt3329rzSkmN0OE0QxlmGJcdBI8rO7le2LvFVNs:OhuUiNrt33sSkmN0OE0QyGJeBwL/G5
MD5:	195ED09E0B4F3B09EA4A3B67A0D3F396
SHA1:	01A250631397C93C4AAB9A777A86E39FD8D84F09
SHA-256:	AEF9FCBB874FC82E151E32279330061F8F22A77C05F583A0CB5E5696654AC456
SHA-512:	B801C03EFA3E8079366A7782D2634A3686D88F64C3C31A03AA5CE71B7BF472766724D209290C231D55DA89DD4F03BD1C0153FFEB514E1D5D408CC2C713CD40
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....K.....!.....> ... ...@....@.. .....>... .@.....S....@.....X...`.....h..... ..... ..H.....text...D... ..... .. `.rsrc.....@.....@..@.relo c.....`.....@..B..... .....H.....|q.....8.....P .....LO.K. 6}.5N..LA..D..|..=T.+.%.O..!@....D.tLl.....8..o...x"...&..C.@"}.dd..CZ..+..4|<.V....Z....=..)...'...n.....*.....K..{....*"..}....*F.~....(H...t<...*6.~.....(I...*.r...p.<...(J.....(J...(K.....*..(L...*F.~....oH...t....*6.~.....oI...*...0..".....u'.....,...(M...t.....,...o....*...0..F..... (.....,r...psN...z..(.....o.....sO...oP.....sO...oQ...*...0..F.....(....-.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.AvalonDock.Themes.Aero.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	86016
Entropy (8bit):	6.028517174831832
Encrypted:	false
SSDEEP:	1536:h71GJ/yox7dMEmjVWm+NdXYoAv/yCJ0xkZthvlQiQaNtPTATK5wsx8NTNf8McZOO:h0J/yox7dMEmjVWm+NdXYoAv/yCJqkZZ
MD5:	15B23FC1C0455E272255A5D05349A4D2
SHA1:	1E865AEEF9BD88ABFBF5AAAA38E487FE96854E16
SHA-256:	1D63F15B0A90CC8766E1F7B12056CF447F319027A3BCD74DDE798C6AB0BECB67
SHA-512:	0D8588259521F6AA096AF9147DB8671678D76F164E5E24013B451F6B4A709CEE2A8A2B6F05C3A44A6E475856A52A6DE8A7DB0E6C14FD0705B05EC4F584E0B45
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V....." ..0..F.....d... ....@.....Wd..O.....$.....c..... ....H.....text....D... ...F..... ..`.rsrc...$.....H.....@..@.rel oc.....N.....@..B.....d.....H.....'.....=...%...c.....0.....(....r...ps.....(....r...ps.....(....r-..ps.....(....rC..ps..... .....(....rY..ps.....(....ro..ps.....(....r...ps.....(....r...ps.....(....r...ps.....(....r...ps.....(....r...ps.....(....r...ps.....(....r '..ps.....(....r?..ps.....(....rW..ps.....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.AvalonDock.Themes.Expression.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	97792
Entropy (8bit):	5.854292152884776
Encrypted:	false
SSDEEP:	1536:CJvB7xXrLqYH4EMcZO0tB+1vB7xXrLqmyOQP09H/SQFlI5R5C6h4Sx+fL7R:EvB7xXrLqYH4yZGvB7xXrLqmyOQPaH/h
MD5:	B6DBB91142AA19E5CBF803F134E39645
SHA1:	94D483ED1C21B40AB5F6D18A6FA3BD3D89B306A7
SHA-256:	76B422FBDD54442AF159CFB1CEC6FEC9BEF0466180F0E32FA65C95D2341C590A
SHA-512:	3614D4C9E0139EC469225B6A5F85DA89847A4201B0844F8FA48F2C1F74586730155F78E563F02907123D99A78F1D29550D97C741AAE2438A8983E0D7CAD6FBB2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..."..Q.....!.....t..... .....@.. .....~.. ..@.....\...O.....H..... ....H.....text....r... ...t..... ..`.rsrc...H.....v.....@..@.rel oc.....\|.....@..B.....H.....z.....%...U..P .....T..s.B=_..L..H.....?.#..S..>...\.%PP_N.....(...w.t{!!B....j.5m.....i%E..... .i[3....d..E#..~f6.o..l$Jw.1%9..a.h.6.(.....(....*...0..$.....{.....,*..}....r...p.s.....(....*&...(....*"..}....*2r...p.s....*..(....*..(....*F.~....(.....&...*J.~.....&...(....*F.~....(....t....*6.~.....(....*F.~.... (....t....*6.~.....(....*F.~....(.....&...*J.~.....&...(....*...0..R.....s.....s.....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.AvalonDock.Themes.Expression.pdb

Process:	C:\Windows\System32\msiexec.exe
File Type:	MSVC program database ver 7.00, 512*63 bytes
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	3.9688996084472437
Encrypted:	false
SSDEEP:	192:Vg0SjVAAA4A6AQAoAtAGAUAriXA0YAoUDx/1uGhcSbGCDDo4xiRt+FSJkBFS2DwB:VZSj2bFNuI7bLRxi+hS
MD5:	40C637D6F6F921B12C89FBD9237242D4
SHA1:	2AED12B85C7ED7D280A0136A5882618A83B9BF4C

SHA-256:	03825E00B1599622F804921B757DC7D8C43E57DC24012C734FD5C0DE0E95DE34
SHA-512:	040DEE406360918D70BA207AEDA0865C63AEDD829CC941E9DF3037BFF68BA83F7233CF6568F2AC75A745B3ACADF5D6A4CECD70F510B5561646D61A6E6490D9 65
Malicious:	false
Preview:	Microsoft C/C++ MSF 7.00...DS.....?... .....>..... ....8~2..... .....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.AvalonDock.Themes.Metro.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	5.591994336390205
Encrypted:	false
SSDEEP:	1536:nE2HNz9vFPPjJo0bsYmdCImlRbtNFG+D3nbDmBwQd:E2HNz9vFPPjy0b3oCImlRbtrbG
MD5:	2ABD211F4C528FBF8076A539663DB49C
SHA1:	5557EBE4853ACC344336515D21388D01F2E07341
SHA-256:	6AB14FA967EEE053A70337E5B6CEF374617425C464D03992A0A93017A633CA77
SHA-512:	30A7DFA68C1A736DD68FE304D32E726EF008E87D5F884DFF3061F8F596189F2A5EAE868EFE560E8FD1E504BFDD8ADE3172A6C950CDCCC59A4164396E49746B 4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V....." ..0..(.....fG... ...`..... .....v... ..@.....G..O....`..(.....HF..... ....H.....text...l'... ...(..... ..`.rsrc...(....`.....*.....@..@.rel oc.....0.....@..B.....EG.....H.....h .....+.....E.....2r...p.s....*..(....*...BSJB.....v4.0.30319.....l.....#~.....#Strings.... ....t...#US.H.....#GUID...X...@...#Blob.....W.....3.....*....*...,....x.....m.~.....~.....~..:.~...S.~...@.....n.A...c.....~...T.~... ..~.....A...&.....A.....A.....M.....M.....!...Q.....V.W.(.V.[.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.AvalonDock.Themes.VS2010.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	83456
Entropy (8bit):	5.6443526329847975
Encrypted:	false
SSDEEP:	1536:e7dsmzcesTEWSRnqS++gGeqGqPjJo0bsXLbPe+Q0T/D2kEcPwVecVArY+H3lCnwO:csmzcesTEWSRnqS++gGeqGqPjy0bSLbi
MD5:	77151F47291647C023298B33DD14A0E5
SHA1:	B8B86BCD77F04E4132391D1A625DE0131DAC1DCC
SHA-256:	ED6721466DEDE7B52E07A4DA06250434C81E430D2ABDC97533D473DC5B693986
SHA-512:	B809E9603C80569A9C25E224A41BF0E9074C930501229F08763D656E7EA707C48A5D91BF20DF450A6C336A44949070EC4C6616CE11064EE46A84754B19CA08C9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V....." ..0..<.....Z... ...`..... .....\n.. ..@.....Y..O....`.....X..... ....H.....text... :... ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....D.....@..B.....Y.....H.....h ..d.....*...-..|X.....2r...p.s....*..(....*...BSJB.....v4.0.30319.....l.....#~.....#Strings.... ....t...#US.L.....#GUID...\.....#Blob.....W.....3.....3.....>.-.....-...P.....|.....^.....w.....d.....f.....+.....x.....f...J. .....f...<.f.....$.....M.....M.....D...Q.....V.|.(.V...

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.AvalonDock.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	412672
Entropy (8bit):	6.067061277105193
Encrypted:	false
SSDEEP:	6144:n96IhTgSKAjtnIMo5sx8xNkxAafrWTkMg6d9A5sa6BBrdLXyESjzqsCTTZLh7x32:LIjGwfrWTzlUJlf
MD5:	E60039EE9A009F0CEE3942A41F0FE67D
SHA1:	0F596519D6446C2E98B4BFE492D314ACBFABBA50
SHA-256:	1D6B69EB3389323D406653D4921E5D5EBDFAE67492AF52221659D0F6D91E7800
SHA-512:	2D1B5D7DE2341CB29F765DA7D46EBDE20182D7E82BB2B129D6F808B1605EB5D39C6496FC8BCB9995004796EAF57E771210A9373F8537D469785C6DF2AAEE803 F
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V....." ..0..B.....`... ..... .....d... ..@.....S`..O.....D....._..... ....H.....text....@... ...B..... ..`.rsrc...D.....D.....@..@.rel oc.....J.....@..B.....`.....H.....`...$_.....~....*.....*.~...*.....*.~....*.....*.~...*.....*.~...*.....*.0..~.....r...p.....(7...s8...(. ...r...p.....(7...s8...(....r7..p.....(7...s8...(....rU..p.....(7...s8...(....rq..p.....(7...s8...(....*...0..9.....s9...(:.....~;...(<...-..(>...-.*. .....s=...~;...(u...*^.r...p(...+. `...(....*^.r...p(...+. 0...(.. ..*^.r...p(...+. ...(....*^.r...p(...+. ...(....*b.r...p(...+..(....(....*..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.DataGrid.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2220032
Entropy (8bit):	6.173738707498935
Encrypted:	false
SSDEEP:	24576:oaBblewQc3DlpxyYR+V+/vwUrBBALQfXnFbsycYkcYLs5SwL2:MuUyYq+7BBAWuK2
MD5:	716392B4286161898 68F0506A69324C9
SHA1:	BD02BF2EE35C822289BAD694EA80C7A4ED886E58
SHA-256:	372D6D3DCFC7D74299A75B894D6AC6E3D6637BD20A25D9700DBCFDB5E3AA19C1
SHA-512:	092CC24DBEF97E8797FE2090808E02A9F16A3B97CE8C29552C34666202CD74EBBFA74EF2CB7473AEBA96C51563F92B1DAEE210FACAE11AE5D1BB6EC6885F7E38
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V....." ..0...!.....!.. ...."..... .....@".....". ..@.....!.O.....".(..... ".....!..... ....H.....text... .!.. ....!..... ..`.rsrc...(.....".....!.....@..@.reloc..... ".....!.....@..B.....!.....H.....I...!.....{....*..{....*V.(.....}.....}....*...0..;.....uq...../(.....{.....{....o...,.(.....{.....{....o....*.*. d3.O) UU.Z(.....{....o....X)UU.Z(.....{....o....X*.0.....r...p.....%..{.....t.....t...-.qt.....t...-.&.+...t...o.....%..{.....u.....u...-.qu.....u...-.&.+...u...o.....(....*..{....*..{....*V.(.....}.....}.... *...0..;.....uv...../(.....{.....{....o...,.(.....{...

C:\Users\user\AppData\Local\Programs\CSC\iRecord\Xceed.Wpf.Toolkit.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1023488
Entropy (8bit):	6.290691935170504
Encrypted:	false
SSDEEP:	24576:qAhWfPHsAmnMsF6xhKlDJz6Nq0voGbklil23vgJ8Xxlo5x4pVbIG6E4:rWMmsF6xhKlDJz6g0vAlilWbo5x4bbIJ
MD5:	926F4086A2D67A546D715C0E71C89E99
SHA1:	EE4F7C398E0D2C8397C4BA931A9F21223766AD0E
SHA-256:	BD04BAC9B8475C4DA1A77A06A90687FBF44E1560A34FDFE59E4DE0E5499F9E62
SHA-512:	F98D49D5A592A4E5F804881D9FAB22BA782850287CD6F046312C597ED7F4168D944D91345AAAF2E3EAE2D220457C55396733128F255F119EC3B9214493EA7BFF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V....." ..0..... ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....h.....,..p.....>. 4.....(J...*2.....oK...*:.....oL...*.0.,.....oM...r...p $.....%...%....oN...t ...*&...oO...*.. (P...*...0.....r!..p.....(Q.....(Q.....sR...(S.....rG..p.1...(Q.....(Q.....1...sR...(S.....rc..p.....(Q.....(Q...(T.....~U.....(Q...r...psR...oV...*F.~....(W.....*J.~..... (X...*F.~....(W....1...*J.~.....1...(X...*....0.....(....-...(Y...*.oZ.....3.([

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord.Common.XmlSerializers.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14336
Entropy (8bit):	4.5986369377786955
Encrypted:	false
SSDEEP:	96:W6JVZbp4pRQbP+cGyrh5LeURQkx26WwacYTZN7+hamBi69zddOSIvuUZjzR5Q7k0:DG8Rakx5p2jaAmSW
MD5:	EB01DFB2B86D9C60889C70573C0EE2FE
SHA1:	4FBEE88E3BDBA865601F1EFD1CC8A2CA85926D5A
SHA-256:	0F48D8F8712D4D9D224B1EE4230D1A8523EBBA67EB67118F09EC57DE7F51643B
SHA-512:	2E6423F37B95E01EAC07CF58DE8F7994339E965247C54DB16B1947A6DF741F4995D9DC53125946907928F79CA5AE4541A25C157EFE48229B28EA0ED2CC2640A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ZE-a.....!.....0.....N... ...`..... ..... ..@.....PN..K...`..... ....H.....text..... ...0..... ..`.rsrc.....`.....2.....@..@.rel oc.....6.....@..B.....N.....H.....T!.....0..E.....(.....(.....i..r...pr...p..(.....1..r=..pr...p...t...(.....(....*6.(.....(....*..(.....(.... .rS..pr...p..(.....(....*6.(.....(....*..0..E.....(.....(.....i..rw..pr...p..(.....1..r...pr...p...t...(.....(....*6.(.....(....*.*..(....*....0.....(....o....&.....(....o....&...(.....86....(.....{.....{....o....9..... (....o...,..(....o.....(....o....&8.....(....o.....(....o.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord.Common.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	92672
Entropy (8bit):	5.775605229580922
Encrypted:	false
SSDEEP:	1536:ocCkAq4267dpdXs3PARQJCKw/wXHrpDLbo3Alm4rpBmBT:ocr4hppsfPJr1HZoJ4r+T
MD5:	AE8FDDB74DF984F1A8F9F7C2E1E7770B
SHA1:	DCD4B1D8B14FB270B47F3EDB433F75FE32D0C7AC
SHA-256:	D228635AE89E98F4B5CF1EE9FA6D3BD30AFF6B82EE271E88708982B2BBF46AFC
SHA-512:	FFD792E0C3CDC38376096FC0EB5F68C1A9E92752602183EF751A8E104BC0D32E9A7F46450D64680D629DD604FA41E4B93C9D0C4098D238F7B34C6FC5AE1205E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...YE-a....." ..0..b.....6.... ....`.....O.....~..... ..... ..H.....text...<`... ...b..... ..`.rsrc.....d.....@..@.reloc..... .....h.....@..B.....H.....0..Y.....~....r...p~ ...o!...&r...p...++.~....o"....(#...%-.&r-..po$....3..*..X..~....o%...2..*6..~.... (....*..0../.....o&.....~....(.....~....(.....~....(.....~....(.....~....o%...-.r/..ps'...z(....-.rc..p~....r...p((...s'...z~.....o"....-3.r...p~....().....r-..p.~....(.....(*.....o+. ..,H.o+...~ ...(,...,6.o+...(-.....(.....~/...(0...,...(1...(2.....

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord.Core.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	26624
Entropy (8bit):	5.607254090547578
Encrypted:	false
SSDEEP:	384:PdXfU9KrJeczJgOaklGvDEEqPg4dvJdRoyd/9jm1Rc11yNQrBjWT2GjZlW3uuvn8:FXoelgLvDENJdvPKydVeiKObuuAtMto
MD5:	80BB6C694E59FD175EC417D41AF0D07A
SHA1:	1D0F225E2CF794A9BB5E046C9CD22A9210432913
SHA-256:	22C5C84A7674F3C1501E93E3694EB4293F6E0ABB729065117BF478F56458D5CE
SHA-512:	B502110C8F6AE121EEE29545BD23F8768F6E8C79F8DD2423E38318397E4B8F8B0F1F40AFBCF4556536C9B697DA646E2CED17128A4D3F1E2FE2683F07688E22A3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....2_....." ..0..`.....b.... ..... ..... ..`.....O.....}..... ....H.....text...._... ...`..... ..`.rsrc.....b.....@..@.reloc..... .....f.....@..B.....D.....H.....>..,?.....r...pQr...ps.....o.....*.rb..pQ.*....0..l.....s.....o.....+$.o.....ri..po....-..(.....o ....o....-....,..o .....*.....0=.....0..].....s!.....?.....o"..... .....(.....%. .....A....%.ri..p.%..(#....%.ri..p.%..(#....($...*....0..C.....C...%.:....o%...%..(&....%..('.....('.....i(.....(....*..0..+. .....i..ia...+.....a`...X....i/....i2.....*V..s(...%.o)....o*...

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecordBO.XmlSerializers.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14336
Entropy (8bit):	4.563924347208004
Encrypted:	false
SSDEEP:	192:UG8xAZGw/2Xdc/PaAmkeKs0J8eTeRYJJ7JP:UGeD6kRBKs0J8eTeRYJRJP
MD5:	2F5E652A07F0F862F54DCA52B01DFC96
SHA1:	F2E105FC6EF7DB8B41D3AA238AFAD8830384F291
SHA-256:	CAF7010A1C7E616E729C5186C09DC027C022B4E01E5E88A6D1347126BC813015
SHA-512:	81462BC884D32C24F4C58AADDCCC84DF07A9C28EFB1A4D59E2D1659673414D2C506519FB891F2491CA007A7B2E02C714A2325DE6E09F4DAFC737CD28B4AED55
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.a.....!.....0.....N... ...`..... ..@.....M..W....`..... ....H.....text...$.... ...0..... ..`.rsrc.....`.....2.....@..@.rel oc.....6.....@..B.....N.....H.....,... .....0..E.....(.....(.....i..r...pr...p..(.....1..r=..pr...p...t....(.....(....*6.(.....(....*..(.....(.... .rS..pr...p..(.....(....*6.(.....(....*..0..E.....(.....(.....i..rw..pr...p..(.....1..r...pr...p...t....(.....(....*6.(.....(....*.*..(....*....0.....(....o....&.....(....o....&...(.....86....(.....{.....{....o....9..... (....o.....,..(....o.....(....o....&8....(....o....(....o.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecordBO.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	291840
Entropy (8bit):	5.890841554152953
Encrypted:	false
SSDEEP:	6144:6F/FxJHkbgIpi3PBaEMiHseFwf618wVyWno9q/JCpt/RYiVJom:oFx+gsi3PRMe6f618wVyWno9WJCpt/RS
MD5:	56F11691FAE4116E8B3DA4B1F05FEE6A
SHA1:	23CD714970CD190D44CA94B4CF1875DC9942DC2B
SHA-256:	AA453DE5DDBADE592538867282E72E3078E055A01A3B4FCDDA7CA86BE8E96C5F
SHA-512:	69691134AE0E63A56F3C50915048B6B363F960787222D6718A01AC15338008AC31B8126DF89D539F834A5D1A0BC99155C9D116A0818A47CF5399DCB27962D321
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.a....." ..0..l.....^.... ....`.....O..... ..... ..H.....text...lj... ...l..... ..`.rsrc.....n.....@..@.reloc..... .....r.....@..B.....@.....H.....d...p}.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.. {....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..s'...}.....(&....r...ps....}%....{.....{%...o.....{%...o(...*2.{%...o/...*..0..A..... {%...-..r...ps....}%...+...{%...o/.....{%....o.....{%.

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7406080
Entropy (8bit):	7.225020139405021
Encrypted:	false
SSDEEP:	98304:XIu2YWJQuW03VYDL074nbLoBaXj99Y9999owe5unv:X1cJQPIYD84nbLoBaXXunv
MD5:	211ED9D4E17D3FED889A73CA6065FC69
SHA1:	D61018BFEF5BC0A8A5755B58CFF56A837E7D0895
SHA-256:	5E15BB9172D7A4F110696DDE2194F29A14E05064C94F09D5D0DC177E456BD37F
SHA-512:	326C83DAF6758139A237CCA45DA52C735D1627D0CAF15F23FDF23453D4F4F1E21FB73DCCBFF6898D2C902D93E9038DB26EBA115D8E61E419CCF5A077B6998D 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....;b.....0...p..B.....~.p.. ....p...@.. .....@ q.....`.....,.p.O.....p..?..... q.....p..... ..... ..H.....text.....p.. ....p..... ..`.rsrc....?....p..@....p..... ..@..@.reloc..... q.....q.....@..B.....`.p.....H.....XMf.....{....*..{....*V.(<.....}:.....};...*...0..;.....u...../(=....{:....{:...o>...,.(?.... {;....{;...o@...*.*. ..'Q)UU.Z(=....{:...oA...X)UU.Z(?....{;...oB...X*.0.....r...p.....%..{:.....-.q.....-.&.+.....oC....%..{;.....-.q.....-.&.+.....oC....(D...*.. {E...*..{F...*V.(<.....}E.....}F...*...0..;.....u...../(=....{E....{E...o>...,.(?....{F..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	15241
Entropy (8bit):	5.158809991932845
Encrypted:	false
SSDEEP:	192:pe7WN75rpIrjJvSJv+JvfJvMJv2tLBOinNnnDVuDuhuvTjpKW6OgjpKw/pvqsJ8T:pMWN7594JvSJv+JvfJvMJv8jJZg
MD5:	C662E9806C1BB7D47C57E00A9E3D0FD2
SHA1:	B6DB08FE6BDD6329662603F3F60A61CFD06044B5
SHA-256:	3DAC730628FD582AC1CFF46D00EA483A241DB7D26B8D2B6830E1F45EC88262E9
SHA-512:	30F70D80431CBFD590E57B4DAE54DA9DEF31E6A8AA854BA259BD32A832AC8E7B472BC28837388B492D500F7DB856E3DE6ABE76C041B748DA9600986CB38FAD 96
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>.<configuration>. <configSections>. <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">. <section name="iRecord_WPF.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false" />. </sectionGroup>. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">. <section name="iRecordBO.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />. </sectionGroup>. </configSections>. <startup>. <supportedRuntime version="v4.0" sku=".NETFramework,Version

C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.manifest

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	43352
Entropy (8bit):	5.2801406252407626

Encrypted:	false
SSDEEP:	384:3x05tue0/jN8fs6xXjaSf2DB+yMZc4gdLiZGSWp20L0P0r2/qb4cEua5qLWvecDV:3x05tue+xJ4ouJ
MD5:	3BC19CF3FA5742E10B559865A10E13E9
SHA1:	A8FE8E39CD15FE0B0BF72BBF1D6D9B5EABC14ECB
SHA-256:	5B7FB25B788D6D2DABC0DA128061451C96496B4936FAA819178D9D4CA90E536D
SHA-512:	A061CDBCC7C270C90EAF6D8724F6FFDE705C0CBF2119C8DA1D237AB87D54E2A9AC37BAC5938242429523E82B3B26653BB02C97A1D7E14874FAFCED5F35098 3A
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<asmv1:assembly xsi:schemaLocation="urn:schemas-microsoft-com:asm.v1 assembly.adaptive.xsd" manifestVersion="1.0" xmlns:asmv1="urn:schemas-microsoft-com:asm.v1" xmlns="urn:schemas-microsoft-com:asm.v2" xmlns:asmv2="urn:schemas-microsoft-com:asm.v2" xmlns:xsi= "http://www.w3.org/2001/XMLSchema-instance" xmlns:co.v1="urn:schemas-microsoft-com:clickonce.v1" xmlns:asmv3="urn:schemas-microsoft-com:asm.v3" xmlns: dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:co.v2="urn:schemas-microsoft-com:clickonce.v2">.. <asmv1:assemblyIdentity name="iRecord_WPF.exe" vers ion="1.2.1.335" publicKeyToken="0000000000000000" language="neutral" processorArchitecture="x86" type="win32" />.. <description asmv2:iconFile="favicon.ico" as mv2:publisher="Corporation Service Company" asmv2:product="iRecord_WPF" asmv2:supportUrl="http://www.erecording.com/Contact/Contact.aspx" xmlns="urn:s chemas-microsoft-com:asm.v1" />.. <application />.. <entryPoint>.. <assemblyIdentit

C:\Users\user\AppData\Local\Programs\CSC\iRecord\jint.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	244736
Entropy (8bit):	5.977636618562963
Encrypted:	false
SSDEEP:	6144:OzrEIEEwbQEUWZl2VMoUaVEzKIWsUCnA:fEDWZlHJaVE7WsUV
MD5:	887E8AA114768A96B932C5F2072FA363
SHA1:	CFB3BD4EAFC587F8AA964709B896E5AD4567B590
SHA-256:	808C4DD85594C828503737C926A40D59158E6FFF255E28B34BC36DA2AE534202
SHA-512:	A950CFB0FD6B0D3D2944E8200719BADC8586EE47AEDA187F04926184451CE457F6475802A98D0B3E73C4A91659C83ABB0A8D84B73E70F578E0F2891118C7FB4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....cX....." ..0..... ....jq.. ..@.....<...O.....l..... ....H.....text...T.... ....`.rsrc...l.....@..@.reloc..... .....@..B.....p.....H.....@...D.....{....*..{ ...*V.(!.....}.....} ...*...0..;.....u...../("....{.....{....o#...,.($....{ ....{ ...o%...*.*. .l.>)UU.Z("....{....o&...X)UU.Z($....{ ...o'...X*.0.....r...p.....%..{.....-.q.....-.&.+.....o(....%..{ .....-.q.....-.&.+.....o(....()...*..{*...*..{+...*V.(!.....} *.....}+...*...0..;.....u...../("....{*....{*...o#...,.($....{+..

C:\Users\user\AppData\Local\Programs\CSC\iRecord\zxcvbn.net.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	708096
Entropy (8bit):	4.504553197898425
Encrypted:	false
SSDEEP:	12288:4cGtMBmTlY2ECxBFrowSyGRkViIWsF/joC+bjzodlNonA1A:1akiEiF5e7sF/jojjYrWn
MD5:	B73BE13CFE7BC8D582D2491F9BC42532
SHA1:	C562DDD4452290763A17419449655E5C62AA0FAF
SHA-256:	109C3185E822D555FD4C800A48D23F2AA00B3C1FFEF02D9E0B7B7EF3C028D7B1
SHA-512:	EBD0F3000437 50EFA5CB9599789B88AC43561C421EC9ABFBAAD96B813883851624DFD03968A1B51B1F960E4FFE76CDCC06E13E21EFD43C777B567D5C9E897C EA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S. T.....!..... ....@..... ..`.....|...O..... .....D..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....\.....#.....(....*.0..3.....~.....(...., r...p.....(....o....s.....~....*.~....*.....*V(....rA..p~....o....*V(....r}.. p~....o....*..{....*"..}....*N.r...p(.....(....*..0..5.....u%.....-.r...ps....*.(.....(....l4.r-..ps....*~....*2.r...p(....*...0../.....u%.....-.r...ps....*.(.....0.r-..ps....*~....*.~....o....*2(.....o....*2(.... .o....*2(.....o....*2(.....o....*2(.....o....*2(.....o ...*.s!...*.~..

C:\Users\user\AppData\Local\Temp\MSI4103.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107008
Entropy (8bit):	6.518267525263852
Encrypted:	false
SSDEEP:	1536:+2UUj/2wsaO1oxlVVCXBlSz0doGxCznBxJFQNCUIsWK6cd4WJpPpxB60q9:dUU6w3lVoxlSz0jUtiNbb4WrPpxB6D9
MD5:	FAB4AA95C57F441B701BE7C2E81EE370

SHA1:	FAD06BB4BEDBF22BCCB2AB105A630F2C4435BBD4
SHA-256:	8AD1084DE9A734B2D5C86F472F671CC324632B3A6CA5AAA0C360D93D4D08E148
SHA-512:	7AB85940F9C6144864FC5B5221EAE30CB5800EE5FA270957109E8F182551806965FE1DFEFFBE655D805AA2BB33B0896725236B4422D3A540D90FD55CE174EF48
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;....k.V.k.V.k.V..bVvk.V..`V.k.V..aVgk.V...Wnk.V...Wok.V...Wik .Vv..Vlk.V.k.V.k.V...Wok.V...W~k.V..lV~k.V.k.V~k.V...W~k.VRich.k.V.....PE..L.....Z.....!.....4..... .....@.....@ ...\.....x.....T.....8...@..... ..(.....text...+..... ..`.rdata...t... ...v.....@..@.data...X"..... ...@....rsrc...x.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Installer\{FD00B0DF-1F5A-4C9D-B945-7531468B5011}\iRecord.ico

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 3 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	15086
Entropy (8bit):	2.5234526920529645
Encrypted:	false
SSDEEP:	96:jlO0lwLkaB6E00Rs6ePvNSgj6yKcsgSDN+D4+j+tl4YfKm36:jlOmwLkkRsnPvNXj/GgSiitl4YS4
MD5:	FE0818EC4474B9852B4C11DF9C4F83A2
SHA1:	2F54D378249F027E1DDBA15BC842500070D5D8FC
SHA-256:	522C7A033DBE1F417B64E380C22B532A21F13FFB1DB6F50EA20C2E810B3CCF53
SHA-512:	15DA768A346FDCC2CAC01DB439A84F4A21E56FED45E04FF028ADF4DC0933DCC887254EC92EE84BAB9BE527661A7E824B899BACFD9954F39BEAF9490DB0DBA758
Malicious:	false
Preview:	......00.... ..%..6... ....%..... .h....6..(...0...`..... .....$..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\CSC\CSC iRecord.lnk

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Archive, ctime=Wed Mar 23 22:26:54 2022, mtime=Sat May 28 02:19:37 2022, atime=Wed Mar 23 22:26:54 2022, length=7406080, window=hide
Category:	dropped
Size (bytes):	1318
Entropy (8bit):	4.910334782140722
Encrypted:	false
SSDEEP:	24:8F9cBg4iHM+R5plch1f8e/TCAuv5okWGAB7Ps/7aB6m:8jcBg9HM+RjlcjhhR+5zWGABg+B6
MD5:	BDEC24375FE4675CD81BFFECBBE84FEC
SHA1:	B2C119006EBF52549B3C83095B032E3D510DE6DA
SHA-256:	7F59A7C07D70DAE992159DD21ED173BC958DDA11758818BCB7AEFC4A5524FB50
SHA-512:	D58F99E97E0511D7E90DB2BB81EBFEBC6D28782CBCD336EFA1C8EF4EEC3648F1DE0D07042D8D31C3F302AC0E17322D7D95C4B0F2F74F33879EAA05AEA8D0BCB5
Malicious:	false
Preview:	L.....F.... ....3.{.?.....Ar...3.{.?....q.....t.:..DG..Yr?.D..U..k0.&...&.....-..Nr...3.....Ar.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny ..Ta.....Y.....f.(.A.p.p.D.a.t.a...B.P.1.....Tb...Local.<.....Ny..Tb.....Y.....L.o.c.a.l.....Z.1.....Tk...Programs..B.....Tb..Tk.....C.....P.r.o.g.r.a .m.s.....J.1.....Tk...CSC.8.....Tk..Tk.....C.S.C.....V.1.....Tu...iRecord.@.....Tk..Tv.....O...i.R.e.c.o.r.d.....I.2...q.wT[. .IRECOR~1.EXE..P.....w T[..Ts.....i.R.e.c.o.r.d._.W.P.F...e.x.e.....p.....-.....o.....h.....C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe....C.S.C. .i.R.e.c.o.r.d.<....\....\....\....\....\....\.L.o.c.a.l.\.P.r.o.g.r.a.m.s.\.C.S.C.\.i.R.e.c.o.r.d.\.i.R.e.c.o.r.d._.W.P.F...e.x.e.....:.....\...I.J.H..

C:\Users\user\Desktop\CSC iRecord.lnk

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Has Working directory, Archive, ctime=Wed Mar 23 22:26:54 2022, mtime=Sat May 28 02:19:37 2022, atime=Wed Mar 23 22:26:54 2022, length=7406080, window=hide
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	4.852890691512487
Encrypted:	false
SSDEEP:	24:8V9cBg4iHM+R5plch1f8eYKTCAuv5okS1GATPLGiPs/7aB6m:8TcBg9HM+RjlcjmYh+5z2GATPLGb+B6
MD5:	94DC3BD02762A941B55CC5FFA73234B0
SHA1:	B2063D79345857B7EF596DC86D6EBADFAAE6ECED
SHA-256:	C306C5CA09137E86955D001AC987419905BCF16C13732AC6A24E1BD51DE22FF9
SHA-512:	EF6BEB1705A42BDD46380F39DDBA9498BDADFEEA6DFB65A43B5F59A54453866742A1AB7003AE54EF2763777BF7F6EFEDC7CCD3AB79BCB40B6B02DE473010A6F4

Malicious:	false
Preview:	L.....F.... ....3.{.?.....Ar...3.{.?....q.....t.:..DG..Yr?.D..U..k0.&...&.....-..Nr...3.....Ar.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny ..Ta.....Y.....f.(.A.p.p.D.a.t.a...B.P.1.....Tb...Local.<.....Ny..Tb.....Y.....L.o.c.a.l.....Z.1.....Tk...Programs..B.....Tb..Tk.....C.....P.r.o.g.r.a .m.s.....J.1.....Tk...CSC.8.....Tk..Tk.....C.S.C.....V.1.....Tu...iRecord.@.....Tk..Tu.....i .i.R.e.c.o.r.d.....l.2...q.wT[. .IRECOR~1.EXE..P.....w T[..Ts.....i.R.e.c.o.r.d._.W.P.F...e.x.e.....p.....-.....o.....h.....C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe....C.S.C. .i.R.e.c.o.r.d.5....\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.r.o.g.r.a.m.s.\.C.S.C.\.i.R.e.c.o.r.d.\.i.R.e.c.o.r.d._.W.P.F...e.x.e.2.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.

C:\Windows\Installer\3e4f5a.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, MSI Installer, Code page: 1252, Title: Installation Database, Subject: iRecord, Author: CSC, Keywords: Installer, Comments: Published by CSC. Email csc-help@cscglobal.com for Questions., Template: Intel;1033, Revision Number: {152FDDD3-47D2-4 FCB-98AD-A21852A58929}, Create Time/Date: Wed Mar 23 20:26:58 2022, Last Saved Time/Date: Wed Mar 23 20:26:58 2022, Number of Pages: 200, Number of Wo rds: 2, Name of Creating Application: Windows Installer XML Toolset (3.11.1.2318), Security: 2
Category:	dropped
Size (bytes):	27500544
Entropy (8bit):	7.960956421946434
Encrypted:	false
SSDEEP:	786432:Odb6YLKPNv/326EPRCg/5RWfIKhdlfFXfHp+A8cVHTfPeEPfUH:OoYOPNH2/zSvHgAbdOn
MD5:	FD867ADA4F27257B97CD1086E2308309
SHA1:	EF352D9BE1BA30D40007D41C396A93D98CE4EA3B
SHA-256:	609053E562CD36056B79D4ACED7547B6EA7F7AF8C0D46AFC08A7FCE52A292909
SHA-512:	B480B12579D995B4F965C411422DF73414184BE824E8711D722D485AFD44BFAAE1610BFD12C0C8E7A949A1DB357304453A0D09FA30983CEA7D50257B4A05DC4
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\3e4f5c.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, MSI Installer, Code page: 1252, Title: Installation Database, Subject: iRecord, Author: CSC, Keywords: Installer, Comments: Published by CSC. Email csc-help@cscglobal.com for Questions., Template: Intel;1033, Revision Number: {152FDDD3-47D2-4 FCB-98AD-A21852A58929}, Create Time/Date: Wed Mar 23 20:26:58 2022, Last Saved Time/Date: Wed Mar 23 20:26:58 2022, Number of Pages: 200, Number of Wo rds: 2, Name of Creating Application: Windows Installer XML Toolset (3.11.1.2318), Security: 2
Category:	dropped
Size (bytes):	27500544
Entropy (8bit):	7.960956421946434
Encrypted:	false
SSDEEP:	786432:Odb6YLKPNv/326EPRCg/5RWfIKhdlfFXfHp+A8cVHTfPeEPfUH:OoYOPNH2/zSvHgAbdOn
MD5:	FD867ADA4F27257B97CD1086E2308309
SHA1:	EF352D9BE1BA30D40007D41C396A93D98CE4EA3B
SHA-256:	609053E562CD36056B79D4ACED7547B6EA7F7AF8C0D46AFC08A7FCE52A292909
SHA-512:	B480B12579D995B4F965C411422DF73414184BE824E8711D722D485AFD44BFAAE1610BFD12C0C8E7A949A1DB357304453A0D09FA30983CEA7D50257B4A05DC4
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSI698A.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	34628
Entropy (8bit):	5.118078176562136
Encrypted:	false
SSDEEP:	768:9kFnbD3Qis35UW1BnzJWBT1UDxWNUfdB2PlRq:6pbD3QvtnalRq
MD5:	9147146C84CCA40DE4F0C747AD88CD38
SHA1:	02F30F727B79A4BF8B1D1A49CB5AEE8379FAC689
SHA-256:	4ADAB5DEBB0E2B8C336374592FDBF15B806EFE31D28D049D30F51BEAFA7AD884
SHA-512:	3BA3BF214EF02F855FEC85E5641F6CF5A8B437D305BAE0C6C1F570E80F6FA837AA41F3E300B17D1A2A4ECE02AE30DEEF445A658875DC26994A4C2BDE874F8E F7
Malicious:	false

Preview:	...@IXOS.@.....@k..T.@.....@.....@.....@.....@.....@.....&.{FD00B0DF-1F5A-4C9D-B945-7531468B5011}..iRecord..RE_iRecord_Installer.msi.@.....@.....@.....@.....i Record.ico..&.{152FDDD3-47D2-4FCB-98AD-A21852A58929}.....@.....@.....@.....@.....@.....@.....@.....@.....iRecord.....Rollback..Rolling back action:..[1]..RollbackCl eanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@4....@.....@.]....&.{5E92A47E-6632-5D72-862B-8813B97D88D9}".01:\Software\CSC\iRecord\installed.@.....@.....@.....@.....@.....&.{93D1A2DE-2F2A-5F74-9143-43A38E185206}+.01:\Software\CSC\iRecord\StartM enuInstalled.@.....@.....@.....@.....@.....&.{6E797130-59F2-463A-85FE-097117D91A20}@.C:\Users\user\AppData\Local\Programs\CSC\iRecord\BarcodeLib.dll.@.....@..... @.....@.....&.{65238290-6439-43E6-981F-DDC4CD2EFD71}A.C:\Users\user\AppData\Local\Programs\CSC\iRecord\ClearScript.dll.@.....@.....@.....@.....&.{2C51C388-6C8D-4115-A9CE-23E781CF82F9}F.C:\Users\

C:\Windows\Installer\SourceHash{FD00B0DF-1F5A-4C9D-B945-7531468B5011}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1688201708529036
Encrypted:	false
SSDEEP:	12:JSbX72FjlHlliAGiLIlHVRpDh/77777777777777777777777vDHFkY7iMXuMz:JTliQI5nyjWwF
MD5:	661D2182AE7223C65AF7EA3E95256FB0
SHA1:	113FB0D801E835F90EA3984B7F235089CEF5EB49
SHA-256:	C53C58B711AC61A165E9624261B6B84F210FA622BFEFA6181E15DCA61D356B0C
SHA-512:	BEFA49563C09C9B36B65F3D281837D5C44570C2674781E8920625D5CD0FB25D1A495410DFCB6FAD1BF2920575E3EB3E4ED08B39E1515F8FFCB0F29357101F53
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5409592879092373
Encrypted:	false
SSDEEP:	48:xllO8PhzuRc06WXJAjT5RXmILGFSRLGsk2P9zLGFS2LGQrc+B:jlBhz1DjTOvSkrB
MD5:	F89310F402C98E88EF16C31298CFAFCE
SHA1:	3B0307E1CF9FED6592E2A0615B170EC1B8EBC4B0
SHA-256:	A470523D93EA90C6EE952AC3D7D0403FB70EAF814688D98F7505702D4A11B213
SHA-512:	CE28771085C40E65EDA1E9CE2DF8974416F7EB0A652B9F6471C45C863406F9CF58AD4D21B4A5200257A29970EDAD386DB308936F69F8666E7A13114B41E66423
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	122558
Entropy (8bit):	5.363512008666216
Encrypted:	false
SSDEEP:	1536:iHzMV+f84vcIH17Yyxkjr0+NVRVle+yjeLWJOQzi7gZFOIKICh/81r8yQ1oXB4HJ:iHHJCoX5CJ
MD5:	B63C0A24A34691D52A59B05C64EE9F9D
SHA1:	82A61A5818040C3E8A5F911C977CBF72F89B8077
SHA-256:	CF340C08B9BFB05FD697148C993AEDB8F0EF99D76C9A81E822841EC98DF901CE
SHA-512:	6EC75C99543758527AD96ACE15018DAF3E4EA11D073F3A9862F28EBA0472B33767108EDD91A36526A8E8B4EA17FDB8B83BCA62FCF8B97F8DAA5327936022CF8 8
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:13:25.847 [3928]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.Hosting, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.863 [3928]: ngen returning 0x00000000..07/23/2020 10:13:25.925 [1900]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.ServerDocument, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.925 [1900]: ngen returning 0x00000000..07/23/2020 10: 13:25.972 [4436]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.v4.0.Framework, Version=10.0.0.00000, Cu lture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /N

C:\Windows\Temp\~DF170E0BA94479F3D4.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF2B6CA314E64CFCAF.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF3D0A1F559312791D.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.1343057751269584
Encrypted:	false
SSDEEP:	24:+BfRJfAebZwLGFipVZyLGiwLGFipVLLGsVO3wGnKZkW+wSgZ+kdPY:+BfRreLGFS2LGjLGFSRLGsk2P9BTY
MD5:	9B0742BA12287E9BFE842F84105DF7B6
SHA1:	58510422344F353ADBE30449A3400FFC665DA614
SHA-256:	C36593156F7E7CE1D5DEA42DF0C15B60C700D7BB747E0C926D044890CB32EF9B
SHA-512:	1ABFB12724C4100BEB2769FC590158B79ECA0C992FA5FA483AFC17FE117A98343A138195644F22978D567344B10B31817F6B7CA1D0FCE159A7C1E235C8DE52C
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF45EDC06B6870A1DF.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5409592879092373
Encrypted:	false

SSDEEP:	48:xllO8PhzuRc06WXJAjT5RXmILGFSRLGsk2P9zLGFS2LGQrc+B:jlBhz1DjTOvSkrB
MD5:	F89310F402C98E88EF16C31298CFAFCE
SHA1:	3B0307E1CF9FED6592E2A0615B170EC1B8EBC4B0
SHA-256:	A470523D93EA90C6EE952AC3D7D0403FB70EAF814688D98F7505702D4A11B213
SHA-512:	CE28771085C40E65EDA1E9CE2DF8974416F7EB0A652B9F6471C45C863406F9CF58AD4D21B4A5200257A29970EDAD386DB308936F69F8666E7A13114B41E66423
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF4EEB3C2A0EFB1260.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.236079713770648
Encrypted:	false
SSDEEP:	48:YllroruyJveFXJjT5qfXmILGFSRLGsk2P9zLGFS2LGQrc+B:IlMr4LTdvSkrB
MD5:	3DBC8F7A16730CCBAEB8E360FCA67E8D
SHA1:	04943FCEEF912897EF0FE04097ADEFDB75B250B5
SHA-256:	31024A1817FCF816ADE3DB4CA5ACF5AD5D72FA039D8FE5ABDB6D538308F15911
SHA-512:	8F705572075A7C3EF36BB5D7CD7A3A28C50ABDE51FB4E76C1EF1A587D544FC6663C0D3CB6738D9776030AAECA66CFE6297B87818EFBA31AAC44A2FBCB3C36194
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF6A82DB31D22522C0.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07555728268566118
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOkGn7ua6uFXLIoVky6lM:2F0i8n0itFzDHFkY7iMXuM
MD5:	CEAEA0012BEA1509133F805F105AB559
SHA1:	8F00C7DAAAFCD082B82EF3722094AD1AE84F6DB8
SHA-256:	EB6D817091BAACF72F15C47FD0FBD605F68588C202F2FBE184B1D6E092F4A151
SHA-512:	1F497D693C5553411D70E2E0EED30D9ABFB259597803A8FA50BB3FEC4686E8156D09073BD1E29F8B033EDDDE59A049C460779A6F02522491DDF70E4940972904
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF9C089A12CD524806.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false

Preview:	.....

C:\Windows\Temp\~DFA264E91955F0F9BB.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFBB1896EEEADE2A86.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5409592879092373
Encrypted:	false
SSDEEP:	48:xllO8PhzuRc06WXJAjT5RXmILGFSRLGsk2P9zLGFS2LGQrc+B:jlBhz1DjTOvSkrB
MD5:	F89310F402C98E88EF16C31298CFAFCE
SHA1:	3B0307E1CF9FED6592E2A0615B170EC1B8EBC4B0
SHA-256:	A470523D93EA90C6EE952AC3D7D0403FB70EAF814688D98F7505702D4A11B213
SHA-512:	CE28771085C40E65EDA1E9CE2DF8974416F7EB0A652B9F6471C45C863406F9CF58AD4D21B4A5200257A29970EDAD386DB308936F69F8666E7A13114B41E66423
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFCC7FD97F2AC2B8FF.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.236079713770648
Encrypted:	false
SSDEEP:	48:YllroruyJveFXJjT5qfXmILGFSRLGsk2P9zLGFS2LGQrc+B:llMr4LTdvSkrB
MD5:	3DBC8F7A16730CCBAEB8E360FCA67E8D
SHA1:	04943FCEEF912897EF0FE04097ADEFDB75B250B5
SHA-256:	31024A1817FCF816ADE3DB4CA5ACF5AD5D72FA039D8FE5ABDB6D538308F15911
SHA-512:	8F705572075A7C3EF36BB5D7CD7A3A28C50ABDE51FB4E76C1EF1A587D544FC6663C0D3CB6738D9776030AAECA66CFE6297B87818EFBA31AAC44A2FBCB3C36194
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFCF776D88B734425A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped

Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFFD954F6991C0C478.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.236079713770648
Encrypted:	false
SSDEEP:	48:YllroruyJveFXJjT5qfXmILGFSRLGsk2P9zLGFS2LGQrc+B:IlMr4LTdvSkrB
MD5:	3DBC8F7A16730CCBAEB8E360FCA67E8D
SHA1:	04943FCEEF912897EF0FE04097ADEFDB75B250B5
SHA-256:	31024A1817FCF816ADE3DB4CA5ACF5AD5D72FA039D8FE5ABDB6D538308F15911
SHA-512:	8F705572075A7C3EF36BB5D7CD7A3A28C50ABDE51FB4E76C1EF1A587D544FC6663C0D3CB6738D9776030AAECA66CFE6297B87818EFBA31AAC44A2FBCB3C36194
Malicious:	false
Preview:	.....>..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, MSI Installer, Code page: 1252, Title: Installation Database, Subject: iRecord, Author: CSC, Keywords: Installer, Comments: Published by CSC. Email csc-help@cscglobal.com for Questions., Template: Intel;1033, Revision Number: {152FDDD3-47D2-4FCB-98AD-A21852A58929}, Create Time/Date: Wed Mar 23 20:26:58 2022, Last Saved Time/Date: Wed Mar 23 20:26:58 2022, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML Toolset (3.11.1.2318), Security: 2
Entropy (8bit):	7.960956421946434
TrID:	• Microsoft Windows Installer (77509/1) 90.64% • Generic OLE2 / Multistream Compound File (8008/1) 9.36%
File name:	RE_iRecord_Installer.msi
File size:	27500544
MD5:	fd867ada4f27257b97cd1086e2308309
SHA1:	ef352d9be1ba30d40007d41c396a93d98ce4ea3b
SHA256:	609053e562cd36056b79d4aced7547b6ea7f7af8c0d46afc08a7fce52a292909
SHA512:	b480b12579d995b4f965c411422df73414184be824e8711d722d485afd44bfaae1610bfd12c0c8e7a949a1db357304453a0d09fa30983cea7d50257b4a05dc41
SSDEEP:	786432:Odb6YLKPNv/326EPRCg/5RWfIKhdlfFXfHp+A8cVHTfPeEPfUH:OoYOPNH2/zSvHgAbdOn
TLSH:	7E573349E9D0DEC6F63A913D5671960CF9AEBC199E40481E76A83B7D2CBB7CC223D005
File Content Preview:	.....>.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 5/12/2021 5:00:00 PM 5/12/2024 4:59:59 PM
Subject Chain	• CN=Corporation Service Company, O=Corporation Service Company, L=Wilmington, S=Delaware, C=US
Version:	3
Thumbprint MD5:	E6741EBF7E64CFFF5457B3C91A3F8772
Thumbprint SHA-1:	AC7B61A59F47F85D7D1E1EB0C36D6877C9D78794
Thumbprint SHA-256:	2697408544DF78FC6982BE9A46C85A95B8EE1C0642A32DE7F04F03D56988FECD
Serial:	3D8865DFBC59BAE29428935D285C7ECE

OLE File "RE_iRecord_Installer.msi"	
Indicators	
Has Summary Info:	
Application Name:	Windows Installer XML Toolset (3.11.1.2318)
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary	
Code Page:	1252
Title:	Installation Database
Subject:	iRecord
Author:	CSC
Keywords:	Installer
Comments:	Published by CSC. Email csc-help@cscglobal.com for Questions.
Template:	Intel;1033
Revion Number:	{152FDDD3-47D2-4FCB-98AD-A21852A58929}
Create Time:	2022-03-23 20:26:58
Last Saved Time:	2022-03-23 20:26:58
Number of Pages:	200
Number of Words:	2
Creating Application:	Windows Installer XML Toolset (3.11.1.2318)
Security:	2

Streams	
Stream Path: \x5DigitalSignature, File Type: data, Stream Size: 6817	
General	
Stream Path:	\x5DigitalSignature
File Type:	data
Stream Size:	6817
Entropy:	7.3699911949108525
Base64 Encoded:	True
Data ASCII:	0 . . . * H . . . . . 0 . . . . 1 . 0 . . . + ... 0 g . . + ... 7 . . . Y 0 W 0 2 . . + ... 7 . . . 0 $ . . . . . F . . . . . 0 ! 0 . . . + ... " S . A . d . : . . 0 . 0 . . . . . B J : ` @ ! . . 0 . . . * H . . . . . 0 r 1 . 0 . . . U . . . . U S 1 . 0 . . . U . . . . D i g i C e r t I n c 1 . 0 . . . U . . . . w w w . d i g i c e r t . c o m 1 1 0 / . . U . . . (D i g i C e r t S H A 2 A s s u r e d I D T i m
Data Raw:	30 82 1a 9d 06 09 2a 86 48 86 f7 0d 01 07 02 a0 82 1a 8e 30 82 1a 8a 02 01 01 31 0b 30 09 06 05 2b 0e 03 02 1a 05 00 30 67 06 0a 2b 06 01 04 01 82 37 02 01 04 a0 59 30 57 30 32 06 0a 2b 06 01 04 01 82 37 02 01 1e 30 24 02 01 02 04 10 f1 10 0c 00 00 00 00 00 c0 00 00 00 00 00 00 46 02 01 00 02 01 00 02 01 00 02 01 00 02 01 00 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 19 9f 8f ff

Stream Path: \x5MsiDigitalSignatureEx, File Type: Non-ISO extended-ASCII text, Stream Size: 20	
General	
Stream Path:	\x5MsiDigitalSignatureEx
File Type:	Non-ISO extended-ASCII text
Stream Size:	20
Entropy:	4.321928094887363
Base64 Encoded:	False
Data ASCII:	r v o . " u : @ F } .
Data Raw:	72 f8 76 6f db b5 22 86 b8 b9 75 f5 3a 40 80 ba 46 f7 7d 0a

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 496	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	496
Entropy:	4.625139990370765
Base64 Encoded:	True
Data ASCII:	. . . . . O h . . . + ' 0 . . . . . x . . . . . , ... \ \ . . . . . h . . . . . t . . . . . | . . . . . I n s t a l l a t i o n D a t a b a s e . . . . . i R e c o r d . . . . . C S C . . . . . I n s t a l e r . . . . . > . . . P u b l i s h e d b y
Data Raw:	fe ff 00 00 06 03 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c0 01 00 00 0e 00 00 00 01 00 00 00 78 00 00 00 02 00 00 00 80 00 00 00 03 00 00 00 a0 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 bc 00 00 00 06 00 00 00 d0 00 00 00 07 00 00 00 18 01 00 00 09 00 00 00 2c 01 00 00 0c 00 00 00 5c 01 00 00

Stream Path: \x16678\x14437\x16830\x16740, File Type: Microsoft Cabinet archive data, 26683823 bytes, 50 files, Stream Size: 26683823	
General	
Stream Path:	\x16678\x14437\x16830\x16740
File Type:	Microsoft Cabinet archive data, 26683823 bytes, 50 files
Stream Size:	26683823
Entropy:	7.998431579133897
Base64 Encoded:	True
Data ASCII:	M S C F . . . .) . . . . . , ... 2 . . . . . T . . . . . F . . . . . w T G . f i l 0 0 8 4 D 5 7 2 C B 1 4 E 4 9 E 1 0 5 B 1 8 8 4 3 2 5 2 E 1 8 4 . . . . . F . . . . 1 E / . f i l 0 6 E B 0 9 0 8 8 3 3 1 7 0 2 1 B A D E 2 1 4 5 6 0 C 3 E 7 D 2 . . 8 . . . d . . . . 1 E . . f i l 1 2 D 7 6 3 6 5 F 3 2 B E A A C 9 9 4 6 D 8 6 1 9 5 6 6 9 6 1 C . . ~ . . . . . B R . f i l 1 A 1 2 0 6 C 5 C 7 F 6 A C F 7 3 1 6 5 B 0 C 6 5 0 9 3 C D 4 7 . . . . . L . .
Data Raw:	4d 53 43 46 00 00 00 00 af 29 97 01 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 32 00 00 00 00 00 00 00 54 0a 00 00 d3 07 01 00 00 46 01 00 00 00 00 00 00 00 77 54 47 83 20 00 66 69 6c 30 30 38 34 44 35 37 32 43 42 31 34 45 34 39 45 31 30 35 42 31 38 38 34 33 32 35 32 45 31 38 34 00 00 1e 04 00 00 46 01 00 00 00 31 45 2f 99 20 00 66 69 6c 30 36 45 42 30 39 30 38 38 33 33 31 37

Stream Path: \x16786\x17522\x17214\x16923\x17574\x16885\x17214\x17574, File Type: MS Windows icon resource - 3 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel, Stream Size: 15086	
General	
Stream Path:	\x16786\x17522\x17214\x16923\x17574\x16885\x17214\x17574
File Type:	MS Windows icon resource - 3 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Stream Size:	15086
Entropy:	2.5234526920529645
Base64 Encoded:	True
Data ASCII:	. . . . . 0 0 . . . . . % . . 6 . . . . % . . . . h . . . 6 . . (. . . 0 . . . ` . . . . . . . . . . $ . . . . . s H o S . m P . y _ / t } } c 4 o S . o S . . f 8 . r H o S . m P . z _ / u b C . d F . k _ c C . [ : . k @ x ] - ` @ . . b B . e F . k ^ b C . s W & ^ ? . . . . e F . . W 6 . r r V $ _ ? . . . . [; . g 9 . . . f 9 W 6 . [; . h ; W 6 . ^ { | b 2 ` A . Z : . l @ W 6 . ` W 7 . Y i < Y 7 . i L . y P W 6 . [. _ @ . y ^ . . Z 9 .
Data Raw:	00 00 01 00 03 00 30 30 00 00 01 00 20 00 a8 25 00 00 36 00 00 00 20 20 00 00 01 00 20 00 a8 10 00 00 de 25 00 00 10 10 00 00 01 00 20 00 68 04 00 00 86 36 00 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff c8 ff ff ff c8 ff ff ff c8 ff ff ff c8 ff ff ff c8 ff ff ff c8 ff ff ff c8 ff ff

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x15103\x17508\x16945\x18485, File Type: PC bitmap, Windows 3.x format, 493 x 58 x 24, Stream Size: 85894	
General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x15103\x17508\x16945\x18485
File Type:	PC bitmap, Windows 3.x format, 493 x 58 x 24
Stream Size:	85894
Entropy:	0.33990775578751065
Base64 Encoded:	True
Data ASCII:	B M O . . . . . 6 . . . (. . . . . : . . . . . P O . . . . . h . . t J . . y R . . . \ \ E . . 7 . . A . . D . . " . > . . = . . 5 . . y ^ (u I I $. 8 . . @ . . @ . . H " . = . . C . . + . . h L . . w] . - . . @ . . ? . . J & . @ . . B . . 1 . . M (. . .) . . H " . Y 8 . \ \ : . R 0 . S 1 . W 5 . S 1 . Q 0 . Z 7 . P - . - . . m P . s & . . L (. X 7 . V 4 . R 0 . V 6 .] < . U 4 . Q . . ^ > . S

General	
Data Raw:	42 4d 86 4f 01 00 00 00 00 00 36 00 00 00 28 00 00 00 ed 01 00 00 3a 00 00 00 01 00 18 00 00 00 00 00 50 4f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x15231\x16684\x17583\x18474, File Type: PC bitmap, Windows 3.x format, 503 x 314 x 24, Stream Size: 474822

General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x15231\x16684\x17583\x18474
File Type:	PC bitmap, Windows 3.x format, 503 x 314 x 24
Stream Size:	474822
Entropy:	0.20500832407365863
Base64 Encoded:	False
Data ASCII:	B M > . . . . . . 6 . . . (. . . . . . : . . . . > . . . .
Data Raw:	42 4d c6 3e 07 00 00 00 00 00 36 00 00 00 28 00 00 00 f7 01 00 00 3a 01 00 00 01 00 18 00 00 00 00 00 90 3e 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x15871\x18088, File Type: MS Windows icon resource - 1 icon, 16x16, 16 colors, Stream Size: 318

General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x15871\x18088
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors
Stream Size:	318
Entropy:	2.034441580055181
Base64 Encoded:	False
Data ASCII:	. . . . (. . . . . . . (. . . . } . . . .
Data Raw:	00 00 01 00 01 00 10 10 10 00 00 00 00 00 28 01 00 00 16 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x16319\x18483, File Type: MS Windows icon resource - 1 icon, 16x16, 16 colors, Stream Size: 318

General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x15103\x17648\x16319\x18483
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors
Stream Size:	318
Entropy:	2.0369361465218003
Base64 Encoded:	False
Data ASCII:	. . . . (. . . . . . . (. . . .
Data Raw:	00 00 01 00 01 00 10 10 10 00 00 00 00 00 28 01 00 00 16 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x15551\x17574\x15295\x16827\x16687\x18480, File Type: MS Windows icon resource - 1 icon, 32x32, 16 colors, Stream Size: 766

General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x15551\x17574\x15295\x16827\x16687\x18480
File Type:	MS Windows icon resource - 1 icon, 32x32, 16 colors
Stream Size:	766
Entropy:	3.3484862648999827
Base64 Encoded:	True
Data ASCII:	. . . . (. . . . . . @ . . . . 3 3 1 . . . . 3 3 2 3 3 3 3 3 3 3 3 3 3 3 3 3 . 3 3 $ D D D D D D D D D D D @ 1 . 2 D D D D D D D D D D D D D D . . 2 D D D D D D @ D D D D D D C . 2 D D D D D D 3 4 D D D D D C . 2 D D D D D @ 3 0 D D D D D . . 3 $ D D D D D 3 4 D D D D D 1 . 3 $ D D D D D @ D D D D D @
Data Raw:	00 00 01 00 01 00 20 20 10 00 00 00 00 00 e8 02 00 00 16 00 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 c0 c0 00 80 80 80 00 00 80 80 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 33

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x15551\x17574\x15551\x17009\x18482, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 16x16, 16 colors, Stream Size: 1078

General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x15551\x17574\x15551\x17009\x18482

General	
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 16x16, 16 colors
Stream Size:	1078
Entropy:	2.8642269548572474
Base64 Encoded:	False
Data ASCII:	....&...........(.......(... ...@.. ..p..............wp...............p...............p..............p..............p..........ww..ww........wp..ww ....wwp.......ww.
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 10 10 10 00 00 00 00 00 28 01 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0 c0 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x16446\x18156\x15518\x17184\x16827\x18468, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 107008

General	
Stream Path:	\x17163\x16689\x18229\x16446\x18156\x15518\x17184\x16827\x18468
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	107008
Entropy:	6.518267525263852
Base64 Encoded:	True
Data ASCII:	MZ..................@...!.L!This program cannot be run in DOS mode....$.......;...kV.kV.kVbVvkV`V.kVaVgkV.WnkV.WokV.WikVv..VlkV.kVkV.WokV.W~kV.lV~kV.k.V~kV.W~kVRich.kV.......................PE..L.....Z..........!..
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 1352

General	
Stream Path:	\x18496\x15167\x17394\x17464\x17841
File Type:	data
Stream Size:	1352
Entropy:	5.026373418516993
Base64 Encoded:	False
Data ASCII:	...................".".".).).).*.*.*.+.+././.0.0.4.4.4.4.4.4.:.:.:.B.B.B.B.B.B.B.B.B.B.B.B.D.D.D.D.D.D.D.D.D.V.V.V.V.].].].].].].f.f.f.f.f..
Data Raw:	07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2f 00 2f 00 30 00 30 00 34 00 34 00 34 00 34 00 34 00 34 00 3a 00 3a 00 3a 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 56 00 56 00 56 00 56 00 5d 00 5d 00 5d 00 5d 00

Stream Path: \x18496\x15518\x16925\x17915, File Type: data, Stream Size: 204

General	
Stream Path:	\x18496\x15518\x16925\x17915
File Type:	data
Stream Size:	204
Entropy:	4.366613484238788
Base64 Encoded:	False
Data ASCII:	.}.~..~...
Data Raw:	e3 01 7d 03 7e 03 7f 03 80 03 81 03 82 03 84 03 86 03 88 03 8a 03 8c 03 8e 03 90 03 93 03 95 03 97 03 99 03 9b 03 9d 03 9f 03 a1 03 a3 03 a5 03 a7 03 a9 03 ab 03 ad 03 af 03 b1 03 b3 03 b5 03 b7 03 b9 03 bb 03 bd 03 bf 03 c1 03 c3 03 c5 03 c7 03 c9 03 cb 03 cd 03 cf 03 d1 03 d3 03 d5 03 d7 03 d9 03 db 03 92 03 00 00 7e 03 7f 03 80 03 81 03 83 03 85 03 87 03 89 03 8b 03 8d 03 8f 03

Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: ASCII text, with very long lines, with CRLF, LF line terminators, Stream Size: 34871

General	
Stream Path:	\x18496\x16191\x17783\x17516\x15210\x17892\x18468
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Stream Size:	34871
Entropy:	5.337644925305309
Base64 Encoded:	True
Data ASCII:	NameTableTypeColumnValue_ValidationNPropertyId_SummaryInformationDescriptionSetCategoryKeyColumnMaxValueNullableKeyTableMinValueIdentifierName of tableName of columnY;NWhether the column is nullableYMinimum value allowedMaximum value allowedFor foreign key
Data Raw:	4e 61 6d 65 54 61 62 6c 65 54 79 70 65 43 6f 6c 75 6d 6e 56 61 6c 75 65 5f 56 61 6c 69 64 61 74 69 6f 6e 4e 50 72 6f 70 65 72 74 79 49 64 5f 53 75 6d 6d 61 72 79 49 6e 66 6f 72 6d 61 74 69 6f 6e 44 65 73 63 72 69 70 74 69 6f 6e 53 65 74 43 61 74 65 67 6f 72 79 4b 65 79 43 6f 6c 75 6d 6e 4d 61 78 56 61 6c 75 65 4e 75 6c 6c 61 62 6c 65 4b 65 79 54 61 62 6c 65 4d 69 6e 56 61 6c 75 65

Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 3964	
General	
Stream Path:	\x18496\x16191\x17783\x17516\x15978\x17586\x18479
File Type:	data
Stream Size:	3964
Entropy:	3.4307240990294923
Base64 Encoded:	False
Data ASCII:	. . . . . e . . . . . 8 . . . . . N . . . . . 6 . . . $ . . . . . o . . . . . B . . . . . o . . . . . ' . . . . . (. . . . . * . . . . . ; . . . . . > . . . . .
Data Raw:	e4 04 00 00 04 00 08 00 05 00 02 00 00 00 00 00 04 00 04 00 06 00 02 00 05 00 0b 00 0b 00 15 00 01 00 65 00 0a 00 01 00 13 00 02 00 0b 00 1a 00 03 00 02 00 08 00 02 00 09 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 0a 00 38 00 0d 00 01 00 0e 00 01 00 03 00 01 00 1e 00 01 00 01 00 4e 00 15 00 01 00 15 00 01 00 36 00 01 00 24 00 01 00 f5 00 01 00 0f 00 01 00 04 00 6f 00

Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 64	
General	
Stream Path:	\x18496\x16255\x16740\x16943\x18486
File Type:	data
Stream Size:	64
Entropy:	3.7244322443615148
Base64 Encoded:	False
Data ASCII:	. . " .) . * . + . / . 0 . 4 . : . B . D . V .] . f . . . . .
Data Raw:	07 00 22 00 29 00 2a 00 2b 00 2f 00 30 00 34 00 3a 00 42 00 44 00 56 00 5d 00 66 00 85 00 8a 00 98 00 9d 00 ab 00 ae 00 af 00 b0 00 b3 00 b9 00 c5 00 d0 00 d9 00 e3 00 ee 00 08 01 12 01 15 01

Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 4104	
General	
Stream Path:	\x18496\x16383\x17380\x16876\x17892\x17580\x18481
File Type:	data
Stream Size:	4104
Entropy:	2.5420624869198116
Base64 Encoded:	False
Data ASCII:	. . . . . " . " . " .) .) .) . * . * . * . + . + . / . / . 0 . 0 . 4 . 4 . 4 . 4 . 4 . 4 . : . : . : . : . B . B . B . B . B . B . B . B . B . B . B . B . D . D . D . D D . D . D . D . D . D . V . V . V . V .] .] .] .] .] .] . f . f . f . f . f . . . . .
Data Raw:	07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 0a 00 0a 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2f 00 2f 00 30 00 30 00 34 00 34 00 34 00 34 00 34 00 34 00 3a 00 3a 00 3a 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 56 00 56 00 56 00 56 00 5d 00 5d 00

Stream Path: \x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	U . V .
Data Raw:	55 03 56 03

Stream Path: \x18496\x16667\x17191\x15090\x17912\x17591\x18481, File Type: data, Stream Size: 36	
General	
Stream Path:	\x18496\x16667\x17191\x15090\x17912\x17591\x18481
File Type:	data
Stream Size:	36
Entropy:	3.3808591137599038
Base64 Encoded:	False
Data ASCII:	. . . . . g . k . . . . . ' ' . . j . l . . . . .
Data Raw:	18 02 18 02 01 80 02 80 67 03 6b 03 00 80 00 80 00 80 14 80 27 81 27 81 10 80 10 80 6a 03 6c 03 00 00 00 00

Stream Path: \x18496\x16786\x17522, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16786\x17522
File Type:	data

General	
Stream Size:	4
Entropy:	2.0
Base64 Encoded:	False
Data ASCII:	C . . .
Data Raw:	43 03 01 00

Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48

General	
Stream Path:	\x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.569235677759417
Base64 Encoded:	False
Data ASCII:	" . # . $. % . & . ' . (.) . . . . x . < .
Data Raw:	22 01 23 01 24 01 25 01 26 01 27 01 28 01 29 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 78 85 dc 85 3c 8f a0 8f c8 99

Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 42

General	
Stream Path:	\x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	42
Entropy:	3.428883414027889
Base64 Encoded:	False
Data ASCII:	" . # . $. * . + . , . - . . . .
Data Raw:	22 01 23 01 24 01 2a 01 2b 01 2c 01 2d 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 fd 7f fe 7f ff 7f 14 85

Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 48

General	
Stream Path:	\x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	48
Entropy:	3.5123194111116605
Base64 Encoded:	False
Data ASCII:	" . $. % . & .) . . . / . 0 . . . . x . . .
Data Raw:	22 01 24 01 25 01 26 01 29 01 2e 01 2f 01 30 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 e8 83 78 85 dc 85 c8 99 94 91 9c 98 00 99

Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: TeX DVI file (\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\(\001C\001G), Stream Size: 208

General	
Stream Path:	\x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486
File Type:	TeX DVI file (\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\3 67\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367 002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002\367\002;\001?\001C\001G)
Stream Size:	208
Entropy:	3.42510992953527
Base64 Encoded:	False
Data ASCII:	. . . . ; . ? . C . G . J . M . P . S . V . Y . \\ . _ . b . e . h . k . n . q . t . w . z . } . . . .
Data Raw:	f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 f7 02 3b 01 3f 01 43 01 47 01 4a 01 4d 01 50 01 53 01 56 01 59 01 5c 01 5f 01

Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: TeX DVI file, Stream Size: 16

General	
Stream Path:	\x18496\x16911\x17892\x17784\x18472
File Type:	TeX DVI file
Stream Size:	16
Entropy:	2.1774212838293647
Base64 Encoded:	False
Data ASCII:	. . . .

General	
Data Raw:	f7 02 00 00 f8 02 00 00 02 80 01 80 00 00 00 80

Stream Path: \x18496\x16918\x17191\x18468, File Type: MIPSEB Ucode, Stream Size: 14	
General	
Stream Path:	\x18496\x16918\x17191\x18468
File Type:	MIPSEB Ucode
Stream Size:	14
Entropy:	1.9502120649147472
Base64 Encoded:	False
Data ASCII:	. 2 . . . . W . . . . .
Data Raw:	01 80 32 00 00 80 00 00 57 03 00 00 00 00

Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: data, Stream Size: 24	
General	
Stream Path:	\x18496\x16923\x17194\x17910\x18229
File Type:	data
Stream Size:	24
Entropy:	3.0424812503605785
Base64 Encoded:	False
Data ASCII:	> . B . . . m . m . n . p . o . o . ; . ? .
Data Raw:	3e 01 42 01 01 80 01 80 6d 03 6d 03 6e 03 70 03 6f 03 6f 03 3b 01 3f 01

Stream Path: \x18496\x16923\x17584\x16953\x17167\x16943, File Type: data, Stream Size: 20	
General	
Stream Path:	\x18496\x16923\x17584\x16953\x17167\x16943
File Type:	data
Stream Size:	20
Entropy:	3.0414460711655216
Base64 Encoded:	False
Data ASCII:	= . q . ; . ? . . . . = . A . . .
Data Raw:	3d 01 71 03 3b 01 3f 01 00 00 00 00 3d 01 41 01 02 80 02 80

Stream Path: \x18496\x16925\x17915\x17884\x17404\x18472, File Type: data, Stream Size: 36	
General	
Stream Path:	\x18496\x16925\x17915\x17884\x17404\x18472
File Type:	data
Stream Size:	36
Entropy:	2.607017709595356
Base64 Encoded:	False
Data ASCII:	c . { . | . z . z . z . . . . .
Data Raw:	63 03 7b 03 7c 03 7a 03 7a 03 7a 03 08 80 0c 80 09 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 80

Stream Path: \x18496\x17100\x16808\x15086\x18162, File Type: data, Stream Size: 8	
General	
Stream Path:	\x18496\x17100\x16808\x15086\x18162
File Type:	data
Stream Size:	8
Entropy:	1.75
Base64 Encoded:	False
Data ASCII:	8 . : . 9 . 9 .
Data Raw:	38 01 3a 01 39 01 39 01

Stream Path: \x18496\x17116\x17778\x16823\x17912, File Type: data, Stream Size: 64	
General	
Stream Path:	\x18496\x17116\x17778\x16823\x17912
File Type:	data
Stream Size:	64
Entropy:	2.433495850947799
Base64 Encoded:	False

General	
Data ASCII:	r . v . = . A . s . w . ; . ? . t . x . . . . . u . u . . . . E . y . . . .
Data Raw:	72 03 76 03 3d 01 41 01 73 03 77 03 3b 01 3f 01 74 03 78 03 00 00 00 00 75 03 75 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 01 79 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x18496\x17163\x16689\x18229, File Type: data, Stream Size: 28

General	
Stream Path:	\x18496\x17163\x16689\x18229
File Type:	data
Stream Size:	28
Entropy:	2.201838730514401
Base64 Encoded:	False
Data ASCII:	1 . 2 . 3 . 4 . 5 . 6 . 7 . . . .
Data Raw:	31 01 32 01 33 01 34 01 35 01 36 01 37 01 01 00 01 00 01 00 01 00 01 00 01 00 01 00

Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 42

General	
Stream Path:	\x18496\x17165\x16949\x17894\x17778\x18492
File Type:	data
Stream Size:	42
Entropy:	3.0532279988878264
Base64 Encoded:	False
Data ASCII:	= . A . E . . . .
Data Raw:	3d 01 41 01 45 01 ec 02 ee 02 f0 02 f2 02 ec 02 f2 02 ee 02 00 00 f0 02 ec 02 ec 02 ed 02 ee 02 ef 02 f3 02 ee 02 f1 02 f1 02

Stream Path: \x18496\x17165\x17380\x17074, File Type: data, Stream Size: 484

General	
Stream Path:	\x18496\x17165\x17380\x17074
File Type:	data
Stream Size:	484
Entropy:	4.159745303864487
Base64 Encoded:	False
Data ASCII:	* . + . , ... ! . % . > . D . I . M . Q . Y .] . g . . . . 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 r r r r r . r r r . r r . r r . r r r r r r . . . . . i . . . U . . U . . U . . . . ' . . . . " . . ? . E . " . . . . . . ? . . . .
Data Raw:	2a 01 2b 01 2c 01 da 01 f0 01 f7 01 0b 02 15 02 1a 02 21 02 25 02 3e 02 44 02 49 02 4d 02 51 02 59 02 5d 02 67 02 86 02 8f 02 a1 02 32 80

Stream Path: \x18496\x17167\x16943, File Type: data, Stream Size: 1000

General	
Stream Path:	\x18496\x17167\x16943
File Type:	data
Stream Size:	1000
Entropy:	4.963836204137411
Base64 Encoded:	False
Data ASCII:	F . I . L . O . R . U . X . [. ^ . a . d . g . j . m . p . s . v . y . | . . . . C . G . J . M . P . S . V . Y . \\ . _ . b . e . h . k . n . q . t w . z . } . . . . ! . " . # . $. % . & . (.) . * . , . - . 0 . 2 . 3 . 5 . 6 . . 9 . : . < . = . > . ? . @ . A . . . . t . . . D . . . .
Data Raw:	46 01 49 01 4c 01 4f 01 52 01 55 01 58 01 5b 01 5e 01 61 01 64 01 67 01 6a 01 6d 01 70 01 73 01 76 01 79 01 7c 01 7f 01 82 01 85 01 88 01 8b 01 8e 01 91 01 94 01 97 01 9a 01 9d 01 a0 01 a3 01 a6 01 a9 01 ac 01 af 01 b2 01 b5 01 b8 01 bb 01 be 01 c1 01 c4 01 c7 01 ca 01 cd 01 d0 01 d3 01 d6 01 d9 01 43 01 47 01 4a 01 4d 01 50 01 53 01 56 01 59 01 5c 01 5f 01 62 01 65 01 68 01 6b 01

Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 144

General	
Stream Path:	\x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	144
Entropy:	4.506971323282542
Base64 Encoded:	False
Data ASCII:	" . # . $. % . & . (.) . . . / . 0 . . D . E . F . G . H . I . J . K . L . M . N . O . P . . . . x . . . . . d @ . (. .

General	
Data Raw:	22 01 23 01 24 01 25 01 26 01 28 01 29 01 2e 01 2f 01 30 01 e8 02 44 03 45 03 46 03 47 03 48 03 49 03 4a 03 4b 03 4c 03 4d 03 4e 03 4f 03 50 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 78 85 dc 85 a0 8f c8 99 94 91 9c 98 00 99 c9 99 19 80 64 80 bc 82 b0 84 40 86

Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 102	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	102
Entropy:	4.505891241724275
Base64 Encoded:	False
Data ASCII:	" . # . $. * . + . , . - . . . % . > . Y . . D . E . F . G . Q . . . . S . R . T . . . . 1 . . . . . d 2
Data Raw:	22 01 23 01 24 01 2a 01 2b 01 2c 01 2d 01 1a 02 25 02 3e 02 59 02 a1 02 44 03 45 03 46 03 47 03 51 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 03 52 03 54 03 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 fd 7f fe 7f ff 7f 14 85 31 80 13 85 11 85 12 85 10 85 19 80 64 80 bc 82 b0 84 32 80

Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: data, Stream Size: 624	
General	
Stream Path:	\x18496\x17548\x17648\x17522\x17512\x18487
File Type:	data
Stream Size:	624
Entropy:	3.9832400678671442
Base64 Encoded:	False
Data ASCII:	; . ? . C . G . J . M . P . S . V . Y . \\ . _ . b . e . h . k . n . q . t . w . z . } . . . . < . @ . D . H . K . N . Q . T . W . Z .] . ` . c . f i . l . o . r . u . x . { . ~ . . . . = . A . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . E . . . . .
Data Raw:	3b 01 3f 01 43 01 47 01 4a 01 4d 01 50 01 53 01 56 01 59 01 5c 01 5f 01 62 01 65 01 68 01 6b 01 6e 01 71 01 74 01 77 01 7a 01 7d 01 80 01 83 01 86 01 89 01 8c 01 8f 01 92 01 95 01 98 01 9b 01 9e 01 a1 01 a4 01 a7 01 aa 01 ad 01 b0 01 b3 01 b6 01 b9 01 bc 01 bf 01 c2 01 c5 01 c8 01 cb 01 ce 01 d1 01 d4 01 d7 01 3c 01 40 01 44 01 48 01 4b 01 4e 01 51 01 54 01 57 01 5a 01 5d 01 60 01

Stream Path: \x18496\x17548\x17905\x17589\x15151\x17522\x17191\x17207\x17522, File Type: data, Stream Size: 504	
General	
Stream Path:	\x18496\x17548\x17905\x17589\x15151\x17522\x17191\x17207\x17522
File Type:	data
Stream Size:	504
Entropy:	3.72341566903778
Base64 Encoded:	False
Data ASCII:	, . , . % . % . % . % . % . % . % . % . % . % . > . > . Y . Y . Y . Y .] .] . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . . . . S . V . & . (. * . , . . . 0 . 2 . 4 . 6 . 8 . ? . A . . . . . [. [. . . . . ? . ? . ? . A . A . A . h . h . h . j . j . j . k . k . k . n . n . o . o . q . q . r . t . v . x . z . | . ~ . . . . x . | . . . .
Data Raw:	2c 01 2c 01 25 02 25 02 25 02 25 02 25 02 25 02 25 02 25 02 25 02 25 02 3e 02 3e 02 59 02 59 02 59 02 59 02 5d 02 5d 02 67 02 8f 02 8f 02 8f 02 8f 02 8f 02 8f 02 8f 02 8f 02 8f 02 53 02

Stream Path: \x18496\x17548\x17905\x17589\x15279\x16953\x17905, File Type: data, Stream Size: 1560	
General	
Stream Path:	\x18496\x17548\x17905\x17589\x15279\x16953\x17905
File Type:	data
Stream Size:	1560
Entropy:	4.20375074879726
Base64 Encoded:	False
Data ASCII:	* . + . , ... ! . ! . % . > . > . > . > . > . > . > . > . > . > . > . > . > . D . I . I . I . M . Q . Y . Y . Y . Y . Y .] .] .] .] .] . g . g . g g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . g . . . . 7 . . . .
Data Raw:	2a 01 2b 01 2c 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 f0 01 f7 01 f7 01 f7 01 f7 01 f7 01 f7 01 f7 01 0b 02 0b 02 0b 02 15 02 15 02 15 02 1a 02 21 02 21 02 25 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 3e 02 44 02 49 02 49 02 49 02 4d 02 51 02 59 02 59 02 59 02 59 02 59 02 5d 02 5d 02 5d 02 5d 02 5d 02 67 02 67 02 67 02 67 02 67 02 67 02

Stream Path: \x18496\x17548\x17905\x17589\x18479, File Type: data, Stream Size: 5590	
General	
Stream Path:	\x18496\x17548\x17905\x17589\x18479
File Type:	data
Stream Size:	5590
Entropy:	4.294693254700807
Base64 Encoded:	True

General	
Data ASCII:	* . * . * . * . * . * . * . + . + . + . + . + . + . + . , . , . , . , . , . , . , . , . , . , ... ! . ! . ! . ! . % . % . % . % . % . % . % . % . % . % . % . % . % . % . % . % . % . % . % . > . > . > . > . > . > . > . > . D . D . D . I . I . I . I . I . I . I . I . I . M . M . M . M . M . M . M . Q . Q . Q . Y . Y . Y . Y . Y . Y . Y
Data Raw:	2a 01 2a 01 2a 01 2a 01 2a 01 2a 01 2b 01 2b 01 2b 01 2b 01 2b 01 2b 01 2b 01 2c 01 2c 01 2c 01 2c 01 2c 01 2c 01 2c 01 2c 01 2c 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 da 01 f0 01 f0 01 f0 01 f0 01 f0 01 f0 01 f0 01 f0 01 f7 01 f7 01 f7 01 f7 01 f7 01 f7 01 f7 01 f7 01 f7 01 0b 02 0b 02 0b 02 0b 02 0b 02 0b 02 0b 02 0b 02 0b 02 0b 02

Stream Path: \x18496\x17630\x17770\x16868\x18472, File Type: data, Stream Size: 32	
General	
Stream Path:	\x18496\x17630\x17770\x16868\x18472
File Type:	data
Stream Size:	32
Entropy:	2.4339645644232903
Base64 Encoded:	False
Data ASCII:	a . a . . . . .
Data Raw:	61 03 61 03 00 00 16 03 16 03 00 00 00 00 00 00 01 02 00 80 02 00 00 80 00 00 00 00 dd 03 de 03

Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: data, Stream Size: 64	
General	
Stream Path:	\x18496\x17753\x17650\x17768\x18231
File Type:	data
Stream Size:	64
Entropy:	4.0725299787950355
Base64 Encoded:	False
Data ASCII:	. . . . . X . Z . [. \\ . ^ . _ . ` . b . d . f . h . a . g . E . Y . 9 . C . 9 . .] . / . . . . c . e . . i .
Data Raw:	16 01 18 02 8c 02 a9 02 be 02 58 03 5a 03 5b 03 5c 03 5e 03 5f 03 60 03 62 03 64 03 66 03 68 03 61 03 67 03 45 01 59 03 39 01 43 03 39 01 ee 02 5d 03 2f 03 ef 02 16 03 63 03 65 03 f7 01 69 03

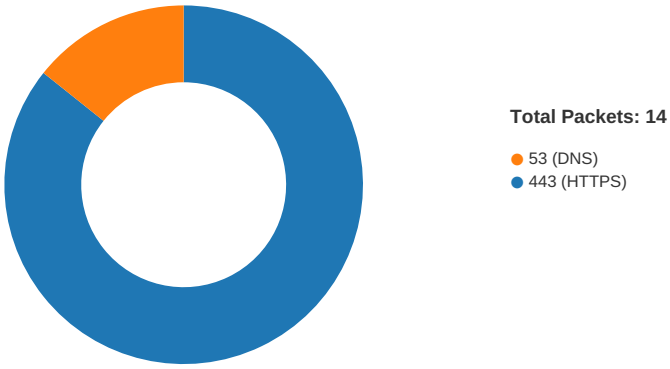
Stream Path: \x18496\x17814\x15340\x17388\x15464\x17828\x18475, File Type: data, Stream Size: 140	
General	
Stream Path:	\x18496\x17814\x15340\x17388\x15464\x17828\x18475
File Type:	data
Stream Size:	140
Entropy:	6.263566163544704
Base64 Encoded:	False
Data ASCII:	j . . . . . b . ; s . . . j @ 7 V 2 - l . T W B a ? . ! 1 W W R | W . U ~ e . . } v . , Y . B . = . R . . i j / u R 0 # r B T
Data Raw:	6a 01 7f 01 82 01 9a 01 a3 01 b5 01 ca 01 00 80 00 80 00 80 00 80 00 80 00 80 00 80 c6 be c7 ab c6 62 e9 00 3b c1 9c 73 d0 9a f9 a3 e2 00 c3 92 6a 9e e4 8e 40 c6 37 56 dd 32 2d 83 6c 1b b7 54 fa 57 42 61 8d c6 f9 90 a4 c4 3f f8 8c 10 f2 8e f6 f9 21 31 b6 57 57 52 7c 57 e0 8a 0b 55 98 e5 7e ae 65 96 02 1a 9c 7d d2 76 1c db 2c 89 fb 59 f6 01 42 09 9e 3d 0f 52 a1 0e 13 69 6a d1 2f 84

Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 36	
General	
Stream Path:	\x18496\x17932\x17910\x17458\x16778\x17207\x17522
File Type:	data
Stream Size:	36
Entropy:	2.9915254351209173
Base64 Encoded:	False
Data ASCII:	. . . A A . 1 . 1 . | . . . . .
Data Raw:	c3 02 e3 02 e8 02 41 80 41 80 d2 80 31 01 31 01 7c 01 e9 02 ea 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x18496\x17998\x17512\x15799\x17636\x17203\x17073, File Type: data, Stream Size: 40	
General	
Stream Path:	\x18496\x17998\x17512\x15799\x17636\x17203\x17073
File Type:	data
Stream Size:	40
Entropy:	3.0477309221191606
Base64 Encoded:	False
Data ASCII:	. . . . . % . % . . . . . : . . . . .
Data Raw:	da 01 1a 02 1a 02 25 02 25 02 e2 01 1f 02 20 02 20 02 3a 02 f4 02 1f 02 20 02 20 02 f5 02 f4 02 1f 00 1f 00 1f 00 f6 02

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:19:55.489953995 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:55.490009069 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:55.490099907 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:55.550364017 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:55.550409079 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:55.645839930 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:55.645987988 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:55.646794081 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:55.646878004 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:55.690267086 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:55.690296888 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:55.690926075 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:55.833671093 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:56.440484047 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:56.484524012 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:56.668869972 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:56.668936968 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:56.669007063 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:56.669004917 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:56.669040918 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:56.669101954 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:56.669110060 CEST	443	49753	205.234.175.175	192.168.2.3
May 27, 2022 20:19:56.669193983 CEST	49753	443	192.168.2.3	205.234.175.175
May 27, 2022 20:19:56.736510992 CEST	49753	443	192.168.2.3	205.234.175.175

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:19:55.363270044 CEST	57421	53	192.168.2.3	8.8.8.8
May 27, 2022 20:19:55.392607927 CEST	53	57421	8.8.8.8	192.168.2.3
May 27, 2022 20:19:55.414859056 CEST	65358	53	192.168.2.3	8.8.8.8
May 27, 2022 20:19:55.441258907 CEST	53	65358	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 20:19:55.363270044 CEST	192.168.2.3	8.8.8.8	0xd879	Standard query (0)	ocp.cscglobal.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 20:19:55.414859056 CEST	192.168.2.3	8.8.8.8	0xced8	Standard query (0)	ocp.cscglobal.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 20:19:55.392607927 CEST	8.8.8.8	192.168.2.3	0xd879	No error (0)	ocp.cscglobal.com	cscglobal.cachefly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:19:55.392607927 CEST	8.8.8.8	192.168.2.3	0xd879	No error (0)	cscglobal.cachefly.net	vip1.g5.cachefly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:19:55.392607927 CEST	8.8.8.8	192.168.2.3	0xd879	No error (0)	vip1.g5.cachefly.net		205.234.175.175	A (IP address)	IN (0x0001)
May 27, 2022 20:19:55.441258907 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	ocp.cscglobal.com	cscglobal.cachefly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:19:55.441258907 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	cscglobal.cachefly.net	vip1.g5.cachefly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:19:55.441258907 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	vip1.g5.cachefly.net		205.234.175.175	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ocp.cscglobal.com

HTTPS Proxied Packets

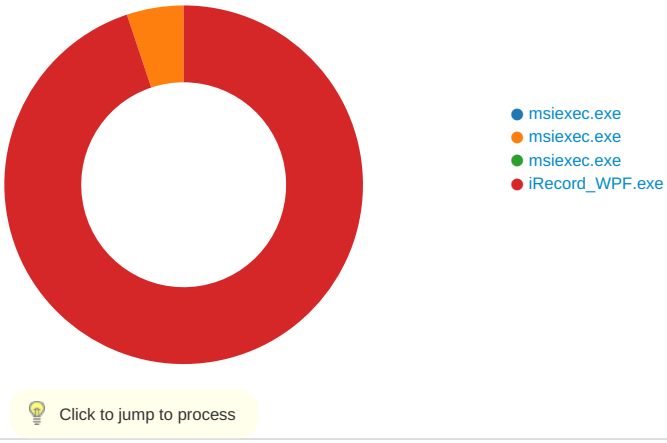
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49753	205.234.175.175	443	C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:56 UTC	0	OUT	GET /cdn/gateway/csc/csc-logo-erecording.png HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ocp.cscglobal.com Connection: Keep-Alive
2022-05-27 18:19:56 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 18:19:56 GMT Content-Type: image/png Content-Length: 4630 Connection: close Access-Control-Allow-Origin: * Cache-Control: max-age=31449600 Expires: Fri, 26 May 2023 18:19:56 GMT X-CFF: B Last-Modified: Fri, 03 May 2019 10:06:03 GMT X-Powered-By: ASP.NET X-CF3: M CF4Age: 0 x-cf-tsc: 1653675597 CF4ttl: 604800.000 X-CF2: M Accept-Ranges: bytes Server: CFS 0215 X-CF1: 15388:fA.cdg1:co:1531782593:cacheB.cdg1-01:M
2022-05-27 18:19:56 UTC	0	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 d2 00 00 00 56 08 06 00 00 00 ba b8 c8 8c 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 ef 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 30 20 37 39 2e 31 36 30 34 35 31 2c 20 32 30 31 37 2f 30 35 2f 30 36 2d 30 31 3a 30 38 3a 32 31 20 20 Data Ascii: PNGIHDRVtEXtSoftwareAdobe ImageReadyqe<iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:56 UTC	1	IN	Data Raw: 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 36 45 33 43 36 42 44 39 31 30 42 46 31 31 45 37 39 44 37 44 45 33 41 38 43 39 42 44 32 44 38 39 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 36 45 33 43 36 42 44 41 31 30 42 46 31 31 45 37 39 44 37 44 45 33 41 38 43 39 42 44 32 44 38 39 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d 70 6d 65 74 61 3e 20 3c 3f 78 70 61 63 6b 65 74 20 65 6e 64 3d 22 72 22 3f 3e a2 a5 bf 33 00 00 0d bd 49 44 41 54 78 da ec 5d 0b b8 15 55 15 5e 88 28 d2 15 14 10 01 41 f1 93 d7 15 f3 c1 4b 0b 12 01 23 03 04 44 50 c2 0c 49 e9 61 5a 52 a4 94 50 9a 25 5f 51 02 19 01 06 4a 82 a0 49 Data Ascii: rom stRef:instanceID="xmp.iid:6E3C6BD910BF11E79D7DE3A8C9BD2D89" stRef:documentID="xmp.did:6E3C6BDA10BF11E79D7DE3A8C9BD2D89"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?> 3IDATx]U^(AK#DPIaZRP%_QJI
2022-05-27 18:19:56 UTC	2	IN	Data Raw: 9b b0 4c 9d 1d e7 46 48 e3 28 c6 02 31 62 e8 ae 70 68 f7 17 55 af 74 1a d2 22 87 f6 48 19 ff 7e 82 f2 60 5d e6 b7 1e bd d6 ee 88 f9 5c 52 40 04 ba ad ec d7 01 c7 df 53 71 14 1a d2 fb cc a5 0e d7 20 5c e7 fc 84 e4 41 7d ba 96 8e bd d1 fd 86 73 08 29 9a cf ac 97 80 7c 17 30 bf ed d0 0e c5 f7 3f 54 f5 4a a7 21 01 0f 3a 5c 83 e2 f4 8f 92 dd fd eb 0b 0c 97 6e f5 30 38 53 6f 74 19 f3 12 0a f2 9a 8e 8b 51 be 3a 32 94 74 d9 2c 60 ba aa 56 ba 90 9d 6a 8e d5 f8 72 72 5b 33 7a 59 94 76 73 0c 72 20 db 76 ae e3 90 6c a5 f4 88 a6 05 e2 c5 54 19 c9 8e b4 90 7e 94 ff 4e 17 27 33 9f a6 ca 74 78 5b 6f d9 94 e2 df 5d 43 71 04 f5 48 88 0f 1b ed 78 6d 7b 19 0a b6 ca 53 86 af 8a 92 ba ce 6b 6e 8a 30 a2 2f d0 a1 e9 20 97 cb 30 ab 7e 1e f2 9d 4d 81 23 a6 bd 63 fb 5f aa 11 a5 10 Data Ascii: LFH(1bphUt"H~`]\R@Sq \A}s)|0?TJ!:\n08SotQ:2t,`Vjrr[3zYvsr vlT~N'3tx[o]CqHxm{Skn0/ 0~M#c_
2022-05-27 18:19:56 UTC	4	IN	Data Raw: ac 63 7b 54 95 d2 0d 97 05 d9 7e 86 e3 53 c8 af ba 28 be e4 cf 65 28 fa c4 ac f3 a6 1d ee 2a 26 fe db 22 ee bd 9c 2a b7 86 81 81 ce 09 69 d3 cd e0 28 81 f3 c0 77 63 b0 c9 19 9e 41 94 27 5b a2 aa 94 6e d8 d6 91 e0 19 5b 6d 38 d7 98 f2 ab ce 93 0d 14 0e 99 67 38 87 82 29 43 3d 86 70 26 83 fc 96 c1 23 78 b5 aa 82 22 c9 a1 dd 05 11 c3 9b f7 63 96 05 15 7b 3e 30 9c 6b 21 93 7c b8 ba b1 eb 43 69 0e f7 3f cf 70 fc 25 55 03 45 d2 86 d4 c4 70 fc 1f 09 c8 82 e1 9e 6d c7 74 2c 7c fe 84 82 72 59 e8 29 c7 51 b0 dd 8b cb 5c cf b4 5b c5 0a 55 03 45 d2 86 74 92 e1 f8 c6 84 e4 41 e8 91 eb 1e 43 30 0c ec 30 fe bc f4 54 43 22 1c 16 c0 c9 86 e3 ba fb b8 22 71 43 aa 69 38 be 35 41 99 46 8a 83 c3 a7 82 2b 5c f4 f7 89 d3 a1 a9 a1 4d 8d 22 bc 8b 42 0d e9 20 4c db 4c d6 4e 58 2e Data Ascii: c{T~S(e(*&"*i(wcA'[n[m8g8)C=p&#x"c{>0k!|Ci?p%UEpmt,|rY)Q\[UEtAC00TC""qCi85AF+\M"B LLNX.

Statistics

Behavior



System Behavior

Analysis Process: msiexec.exe PID: 6632, Parent PID: 3632

General

Target ID:	0
Start time:	20:19:00
Start date:	27/05/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\RE_iRecord_Installer.msi"
Imagebase:	0x7ff62e2a0000
File size:	66048 bytes

MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6692**, Parent PID: **568**

General

Target ID:	1
Start time:	20:19:02
Start date:	27/05/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff62e2a0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	122464	94	30 35 2f 32 37 2f 32 30 32 32 20 32 30 3a 31 39 3a 31 38 2e 32 37 30 20 5b 36 36 39 32 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	05/27/2022 20:19:18.270 [6692]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFC6090BEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFC6090BBC6	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6960**, Parent PID: **6692**

General

Target ID:	5
Start time:	20:19:09
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 5E1FB7355188E254823CE3315A71CFED C
Imagebase:	0xf0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iRecord_WPF.exe PID: **7048**, Parent PID: **6692**

General

Target ID:	17
Start time:	20:19:47
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe
Imagebase:	0x810000
File size:	7406080 bytes
MD5 hash:	211ED9D4E17D3FED889A73CA6065FC69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D52CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D52CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WPFE457.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B0EC055	GetTempFileNameW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C371B4F	WriteFile
unknown	4096	534	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C371B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	8174	end of file	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D505705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4603DE	ReadFile
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	4095	success or wait	1	6D50CA54	ReadFile
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	8174	end of file	1	6D50CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D50CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C371B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C371B4F	ReadFile
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	4096	success or wait	1	6C371B4F	ReadFile
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	4096	end of file	1	6C371B4F	ReadFile
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	8174	end of file	1	6D505705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatioaec034ca#\71c166f74def9b205fafc80dbd0c1015\PresentationFramework.Aero2.ni.dll.aux	unknown	1252	success or wait	1	6D4603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WPFE457.tmp	unknown	0	success or wait	1	6C371B4F	ReadFile
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Users\user\AppData\Local\Programs\CSC\iRecord\iRecord_WPF.exe.config	unknown	8174	end of file	1	6D505705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WPFE457.tmp	unknown	33	success or wait	1	693A8246	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WPFE457.tmp	unknown	8	success or wait	1	693A8246	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WPFE457.tmp	unknown	8	success or wait	4	693A8246	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WPFE457.tmp	unknown	8	success or wait	1	693A985A	unknown

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly